Important: As of December 31, 2021, Coveo Enterprise Search (CES) version 7 reached end of life and is no longer supported by Coveo. We continued to offer technical support to all active CES customers up until December 31, 2021.

Coveo Platform 7.0
Administrator Guide
Notice

The content in this document represents the current view of Coveo as of the date of publication. Because Coveo continually responds to changing market conditions, information in this document is subject to change without notice. For the latest documentation, visit our website at www.coveo.com.

© Coveo Solutions Inc., 2013

Coveo is a trademark of Coveo Solutions Inc. This document is protected by intellectual property laws and is subject to all restrictions specified in the Coveo Customer Agreement.

Document part number: PM-070323-EN
Publication date: 9/19/2023
# Table of Contents

1. Introduction .................................................................................................................. 2

2. Coveo Platform Hardware and Software Requirements ................................................. 3
   2.1 Index of up to 5 Million Documents (Minimum Requirements) .................................. 3
   2.2 Index From 5 to 20 Million Documents .................................................................... 3
   2.3 Index From 20 to 40 Million Documents ................................................................... 4
   2.4 Index From 40 to 80 Million Documents ................................................................... 4
   2.5 Operating System Compatibility ............................................................................. 5
   2.6 Index Size ................................................................................................................ 6
   2.7 Non Index Files ....................................................................................................... 6
   2.8 RAID Configuration ............................................................................................... 6
   2.9 Near Real-Time Indexing Disk ................................................................................ 7
   2.10 Third-Party Software Requirement ....................................................................... 7
   2.11 TLS/SSL Compatibility ......................................................................................... 8
   2.12 Relation Between CES Features and Hardware Resources ..................................... 8
   2.13 RAID Type Comparison and Recommendations .................................................... 9
   2.14 Virtualized Server Guidelines ............................................................................... 10
      2.14.1 Guidelines ..................................................................................................... 10

3. Deployment .................................................................................................................... 12
   3.1 Coveo Platform Deployment Overview .................................................................... 12
   3.2 Coveo Scalability Model ......................................................................................... 14
      3.2.1 One Server Configurations ............................................................................. 14
      3.2.2 Larger Number of Documents: Add a Slice ..................................................... 14
      3.2.3 More Queries: Add Mirror and Front-End Servers ......................................... 15
      3.2.4 Heavy Document Conversion: Add Remote Converter Servers ...................... 16
      3.2.5 Indexes in Various Locations: Set Up a Geographically Distributed Index (GDI) ......................................................................................................................... 17
      3.2.6 About Index Slices ........................................................................................... 18
      3.2.7 About Mirror Servers ...................................................................................... 18
      3.2.8 About Geographically Distributed Indexing ..................................................... 20
         3.2.8.1 Setting up Geographically Distributed Indexing .......................................... 21
         3.2.8.2 Setting up Geographically Distributed Indexing Using a Mirror .................. 22
4.13 Creating a Custom Color Scheme for the Outlook Sidebar in the Windows Registry .......... 172
4.14 Microsoft SharePoint Integration .................................................................................. 174
  4.14.1 Integrating the Coveo .NET Search Box in My Site for SharePoint 2013 and 2016 .......... 174
  4.14.2 Activating or Deactivating the Coveo .NET Search Box in a SharePoint Site ............... 176
  4.14.3 Manually Configuring a .NET Search Interface Claims SSO for an On-Premises SharePoint .... 178
    4.14.3.1 SharePoint Server Configuration ................................................................. 179
    4.14.3.2 Coveo .NET Front-End Server Configuration .................................................. 182
  4.14.4 Configuring the Claims-Aware Coveo Search Application ........................................ 183
    4.14.4.1 Step 1: Enabling Claims Authentication on the Coveo Search Site ....................... 184
    4.14.4.2 Step 2: Creating the Coveo Relying Party Trust .............................................. 186
    4.14.4.3 Step 3: Editing Claims Rules for the Coveo Relying Party Trust ............................ 186
    4.14.4.4 Step 4: Editing Claims Rules for the SharePoint Relying Party Trust ..................... 186
    4.14.4.5 Step 5: Configuring the Coveo Service Account for ADFS Identity Delegation ............ 187
    4.14.4.6 Step 6: Performing the First-Time Setup on the Coveo Search Site ....................... 187
  4.14.5 Configuring SharePoint Search Scopes ....................................................................... 187

5. Migration ............................................................................................................................. 193
  5.1 Coveo Platform 6 to 7 Migration Overview ..................................................................... 193
  5.2 Configuring a Coveo .NET Front-End 12 Server to Use a CES 6.5 Back-End Server ............ 195
    5.2.1 Configuring the Front-End to Use a CES 6.5 Back-End .......................................... 195
    5.2.2 Editing web.config Files to Enable the Use of the .NET Interface Editor .................. 196

6. CES Moving Scenarios ........................................................................................................ 199
  6.1 Moving the CES Configuration Folder ............................................................................ 200
  6.2 Moving the Index to a Different Hard Disk Drive ......................................................... 202
  6.3 Moving the Index to Another Server .............................................................................. 203
  6.4 Moving Skins .................................................................................................................. 204
  6.5 Changing the Index Folder in the CES Configuration File .............................................. 205
  6.6 About the Index Backup Feature .................................................................................... 205
    6.6.1 Backing Up the Index From the Administration Tool .............................................. 206
    6.6.2 Backing Up the Index With a PowerShell Script .................................................... 208
    6.6.3 Restoring an Index Backup ...................................................................................... 213
  6.7 Manually Backing Up and Restoring the Index .............................................................. 215

www.coveo.com
6.8 Backing Up and Restoring the CES Configuration Files .................................................. 216

7. Security ........................................................................................................................................ 218
  7.1 At Indexing Time .................................................................................................................. 219
  7.2 At Query Time ..................................................................................................................... 219
  7.3 Security Cache Update ......................................................................................................... 220
  7.4 Security Control Levels in CES .......................................................................................... 220
  7.5 Security Model Types .......................................................................................................... 222
  7.6 Permission Levels and Sets .................................................................................................. 223
  7.7 About the CES Service Logon Account .............................................................................. 223
    7.7.1 Setting or Changing the CES Service Logon Account .................................................... 225
    7.7.2 CES Service Logon Account Best Practices .................................................................. 226
  7.8 Modifying the CES Log On Account .................................................................................. 227
  7.9 Who Has Access to the Administration Tool? ...................................................................... 228
  7.10 Ports Used By the Coveo Platform .................................................................................... 229
  7.11 About the CES Service Port .............................................................................................. 230
  7.12 Coveo REST Search API 8.0 ............................................................................................. 230
  7.13 About the Coveo Search Web Service .............................................................................. 231
  7.14 About the Coveo Admin Service ...................................................................................... 231
    7.14.1 Validating That the Coveo Admin Service Is Running ................................................ 232
  7.15 CES and Anti-Virus Software ............................................................................................ 232
    7.15.1 CES/Virus Considerations .......................................................................................... 233
    7.15.2 Possible Interferences .................................................................................................. 233
    7.15.3 Recommendations ....................................................................................................... 233
    7.15.4 Scanning Coveo Files While the Index Is in Read-Only Mode ..................................... 234
    7.15.5 Scanning Coveo Files While the CES Service Is Stopped ........................................... 235
  7.16 About Search Security Certificate ..................................................................................... 235
    7.16.1 Deployed Search Security Configuration ..................................................................... 236
    7.16.2 Manually Configuring Search Security Certificate ....................................................... 237
      7.16.2.1 Local Front-End ...................................................................................................... 238
      7.16.2.2 Remote Front-End .................................................................................................. 238
      7.16.2.3 Remote Front-End querying multiple Coveo instances .......................................... 239
<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>7.16.2.4 Geographically distributed indexing (GDI)</td>
<td>239</td>
</tr>
<tr>
<td>7.16.2.5 SharePoint integration</td>
<td>240</td>
</tr>
<tr>
<td>7.16.3 Editing a Certificate Whitelist</td>
<td>240</td>
</tr>
<tr>
<td>7.16.4 Finding the Thumbprint of a Certificate</td>
<td>241</td>
</tr>
<tr>
<td>7.17 Sitecore Connector Security Update</td>
<td>243</td>
</tr>
<tr>
<td><strong>8. Coveo Platform On-Premises Products</strong></td>
<td>245</td>
</tr>
<tr>
<td>8.1 Using the CES Console</td>
<td>246</td>
</tr>
<tr>
<td>8.2 Starting the CES Service</td>
<td>248</td>
</tr>
<tr>
<td>8.3 Stopping the CES Service</td>
<td>251</td>
</tr>
<tr>
<td>8.4 Identifying the Coveo Enterprise Search Version</td>
<td>252</td>
</tr>
<tr>
<td>8.5 Checking for Available Coveo Enterprise Search Updates</td>
<td>253</td>
</tr>
<tr>
<td>8.6 CES Administration Tool</td>
<td>254</td>
</tr>
<tr>
<td>8.6.1 Opening the Administration Tool</td>
<td>256</td>
</tr>
<tr>
<td>8.6.2 Navigating in the Administration Tool</td>
<td>257</td>
</tr>
<tr>
<td>8.6.3 Administration Tool - Status Tab</td>
<td>257</td>
</tr>
<tr>
<td>8.6.3.1 Administration Tool - Overview Menu</td>
<td>258</td>
</tr>
<tr>
<td>8.6.3.1.1 What Is a Transaction?</td>
<td>259</td>
</tr>
<tr>
<td>8.6.3.1.2 Forcing the Commit of a Transaction</td>
<td>260</td>
</tr>
<tr>
<td>8.6.3.1.3 Reviewing CES Recommended Tasks</td>
<td>260</td>
</tr>
<tr>
<td>8.6.3.2 Administration Tool - Details Menu</td>
<td>261</td>
</tr>
<tr>
<td>8.6.3.2.1 Toggling the Index Between the Read-Write and Read-Only Modes</td>
<td>263</td>
</tr>
<tr>
<td>8.6.3.2.2 What Is a Security Cache?</td>
<td>264</td>
</tr>
<tr>
<td>8.6.3.2.2.1 External Security Cache</td>
<td>265</td>
</tr>
<tr>
<td>8.6.3.2.3 Refreshing Security Caches</td>
<td>266</td>
</tr>
<tr>
<td>8.6.3.2.4 Disabling or Enabling Queries</td>
<td>268</td>
</tr>
<tr>
<td>8.6.3.2.5 Disabling or Enabling Indexing</td>
<td>269</td>
</tr>
<tr>
<td>8.6.4 Administration Tool - Index Tab</td>
<td>269</td>
</tr>
<tr>
<td>8.6.4.1 About the Index</td>
<td>269</td>
</tr>
<tr>
<td>8.6.4.2 About the Index Self-Optimization Process</td>
<td>270</td>
</tr>
<tr>
<td>8.6.4.3 About Foreign Keys</td>
<td>271</td>
</tr>
<tr>
<td>8.6.4.4 About Index Resilience</td>
<td>272</td>
</tr>
</tbody>
</table>
8.6.4.5 Query Correction Feature ................................................................. 273
8.6.4.5.1 Influencing the Word Corrector Lexicon Algorithm .......................... 275
8.6.4.6 Administration Tool - Sources and Collections Menu .......................... 276
8.6.4.6.1 What Is the Difference between a Collection and a Source? .......... 276
8.6.4.6.2 Adding a Collection ......................................................................... 277
8.6.4.6.3 Renaming a Collection .................................................................... 278
8.6.4.6.4 Modifying Collection Permissions .................................................. 279
8.6.4.6.5 What Should Be the Size of a Collection? ....................................... 281
8.6.4.6.6 Adding a Source .............................................................................. 281
8.6.4.6.7 Toggling Live Monitoring for a Source ........................................ 282
8.6.4.6.8 Applying an Action to a Collection or a Source ............................. 283
8.6.4.6.9 Incremental Refresh vs Full Refresh vs Rebuild ............................ 285
8.6.4.6.10 What Are the Possible Statuses of a Source? ................................. 285
8.6.4.6.11 What Is the Difference between Save and Save and Start? ........... 286
8.6.4.6.12 What Should Be the Size of a Source? .......................................... 287
8.6.4.6.13 What Are the Source Properties? ................................................ 287
8.6.4.6.14 What Information Is Displayed in the Status Page? ..................... 289
8.6.4.6.15 Modifying General Source Parameters ........................................ 292
8.6.4.6.16 Adding or Modifying Source Filters ........................................... 295
8.6.4.6.17 Modifying Source Security Permissions ....................................... 297
8.6.4.6.17.1 Modifying the permissions ......................................................... 298
8.6.4.6.17.2 Mapping the security permissions of a Web source ................. 300
8.6.4.6.18 Indexing Secure Web Pages Using Forms ...................................... 300
8.6.4.6.18.1 Retrieving the form parameters from a website ....................... 301
8.6.4.6.18.2 Entering the form parameters manually ................................... 303
8.6.4.6.18.3 Deleting the authentication cookies ........................................ 303
8.6.4.6.19 Managing Single Documents Within Local/Network or Web Sources .......................... 303
8.6.4.6.20 Modifying Advanced Source Parameters .................................... 305
8.6.4.6.21 What Are Wildcards? ................................................................. 308
8.6.4.6.22 About Incremental Refresh and Live Monitoring ....................... 308
8.6.4.6.23 Limiting the Crawling Depth ....................................................... 309

www.coveo.com
<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>8.6.4.6.23.1 Indexing only the main folders or sites</td>
<td>309</td>
</tr>
<tr>
<td>8.6.4.6.23.2 Limiting the crawling depth by level</td>
<td>310</td>
</tr>
<tr>
<td>8.6.4.6.24 What Is the Difference Between ANSI and UTF-8 URI Formats?</td>
<td>311</td>
</tr>
<tr>
<td>8.6.4.6.25 Manually Indexing Sources</td>
<td>311</td>
</tr>
<tr>
<td>8.6.4.7 Administration Tool - Top Results Menu</td>
<td>312</td>
</tr>
<tr>
<td>8.6.4.7.1 Adding Top Results to a CES Index</td>
<td>313</td>
</tr>
<tr>
<td>8.6.4.7.1.1 Adding Top Results from the Index Browser</td>
<td>314</td>
</tr>
<tr>
<td>8.6.4.7.1.2 Adding Top Results from the Top Results page</td>
<td>314</td>
</tr>
<tr>
<td>8.6.4.7.2 Managing Top Results in a CES Index</td>
<td>316</td>
</tr>
<tr>
<td>8.6.4.8 Administration Tool - Ranking Menu</td>
<td>317</td>
</tr>
<tr>
<td>8.6.4.8.1 Best Practices for Ranking Optimization</td>
<td>317</td>
</tr>
<tr>
<td>8.6.4.8.2 What Is Collaborative Rating?</td>
<td>319</td>
</tr>
<tr>
<td>8.6.4.8.3 Configuring Collaborative Rating</td>
<td>319</td>
</tr>
<tr>
<td>8.6.4.8.4 Customizing Search Results Ranking</td>
<td>321</td>
</tr>
<tr>
<td>8.6.4.8.5 Index Ranking Phases</td>
<td>326</td>
</tr>
<tr>
<td>8.6.4.9 Phase 1: Term weighting</td>
<td>327</td>
</tr>
<tr>
<td>8.6.4.10 Phase 2: Document weighting</td>
<td>328</td>
</tr>
<tr>
<td>8.6.4.11 Phase 3: Collaborate ranking</td>
<td>328</td>
</tr>
<tr>
<td>8.6.4.12 Phase 4: Term frequency–inverse document frequency (TF-IDF)</td>
<td>328</td>
</tr>
<tr>
<td>8.6.4.13 Phase 5: Adjacency ranking</td>
<td>329</td>
</tr>
<tr>
<td>8.6.4.13.1 Troubleshooting Ranking</td>
<td>329</td>
</tr>
<tr>
<td>8.6.4.14 Thesaurus Menu</td>
<td>331</td>
</tr>
<tr>
<td>8.6.4.14.1 Thesaurus Best Practices</td>
<td>331</td>
</tr>
<tr>
<td>8.6.4.14.2 Adding Thesaurus Entries From the Administration Tool</td>
<td>332</td>
</tr>
<tr>
<td>8.6.4.14.3 Creating or Modifying a Thesaurus XML File</td>
<td>335</td>
</tr>
<tr>
<td>8.6.4.14.4 Importing a Thesaurus XML File in CES</td>
<td>337</td>
</tr>
<tr>
<td>8.6.4.14.5 Refreshing the Thesaurus</td>
<td>338</td>
</tr>
<tr>
<td>8.6.4.15 Administration Tool - Mirrors Menu</td>
<td>338</td>
</tr>
<tr>
<td>8.6.4.15.1 Adding a Mirror Server</td>
<td>338</td>
</tr>
<tr>
<td>8.6.4.15.2 Adding an Index Slice to the Master Server</td>
<td>342</td>
</tr>
<tr>
<td>8.6.4.15.3 Applying an Action to a Mirror</td>
<td>344</td>
</tr>
</tbody>
</table>
8.7.1.3 Using the Security Browser ................................................................. 383
8.7.2 Administration Tool - Reports Tab .......................................................... 386
  8.7.2.1 What Is the Difference between Reports and Logs? ................................. 386
  8.7.2.2 What Information Is Displayed in the Query History? ............................... 386
  8.7.2.3 What Information Is Displayed in the Index History? ................................. 388
  8.7.2.4 What Information Is Displayed in the Document Statistics Page? .................... 389
  8.7.2.5 Displaying Reports .................................................................................. 390
  8.7.2.6 Modifying the Report Settings ................................................................. 391
  8.7.2.7 Exporting Query/Index History in Excel Format .......................................... 392
  8.7.2.8 Why Is the Query/Index History Empty? ................................................... 393
8.7.3 Administration Tool - Logs Tab .................................................................... 393
  8.7.3.1 What Information Is Displayed in the System Log? ...................................... 393
  8.7.3.2 What Information Is Displayed in the Query Log? ....................................... 395
  8.7.3.3 What Information Is Displayed in the Index Log? ........................................ 398
  8.7.3.4 Displaying Logs ....................................................................................... 401
  8.7.3.5 Modifying the Log Settings ....................................................................... 402
  8.7.3.6 Why Is the Query and Index Log Empty? .................................................... 404
  8.7.3.7 Reviewing Administration Changes ........................................................... 404
8.7.4 Administration Tool - Configuration Tab ...................................................... 405
  8.7.4.1 Administration Tool - Security Menu ....................................................... 406
    8.7.4.1.1 About Administration Roles ................................................................. 406
      8.7.4.1.1.1 Administration Role Feature Comparison ........................................... 406
      8.7.4.1.1.2 Administration Role Short Descriptions ............................................ 410
    8.7.4.1.2 Assigning Users to Administration Roles .............................................. 412
    8.7.4.1.3 What Is an Impersonator? .................................................................... 415
    8.7.4.1.4 Granting Impersonator Privileges ......................................................... 415
    8.7.4.1.5 What Are Security Providers? ............................................................... 417
    8.7.4.1.6 Adding or Modifying a Security Provider .............................................. 417
    8.7.4.1.7 Restarting a Security Provider .............................................................. 418
    8.7.4.1.8 Restarting a Security Provider .............................................................. 419
    8.7.4.1.9 Adding a User Identity ......................................................................... 420
<table>
<thead>
<tr>
<th>Section</th>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>8.7.4.7.8</td>
<td>Adding a Field to Search On</td>
<td>499</td>
</tr>
<tr>
<td>8.7.4.7.9</td>
<td>Adding a Facet Field</td>
<td>500</td>
</tr>
<tr>
<td>8.7.4.7.10</td>
<td>Adding a Sorting Field</td>
<td>502</td>
</tr>
<tr>
<td>8.7.4.7.11</td>
<td>Managing Display Fields</td>
<td>504</td>
</tr>
<tr>
<td>8.7.4.8</td>
<td>Administration Tool - Field Aliases Menu</td>
<td>505</td>
</tr>
<tr>
<td>8.7.4.8.1</td>
<td>Adding a Field Alias Set</td>
<td>506</td>
</tr>
<tr>
<td>8.7.4.8.2</td>
<td>Managing Field Aliases</td>
<td>506</td>
</tr>
<tr>
<td>8.7.4.8.2.1</td>
<td>Adding a new field alias</td>
<td>507</td>
</tr>
<tr>
<td>8.7.4.8.2.2</td>
<td>Modify an existing field alias</td>
<td>507</td>
</tr>
<tr>
<td>8.7.4.8.2.3</td>
<td>Deleting an existing field alias</td>
<td>507</td>
</tr>
<tr>
<td>8.7.4.9</td>
<td>Administration Tool - XML Menu</td>
<td>508</td>
</tr>
<tr>
<td>8.7.4.9.1</td>
<td>Adding an XML Document Definition</td>
<td>508</td>
</tr>
<tr>
<td>8.7.4.9.2</td>
<td>Adding and Modifying XML Elements to a Document Definition</td>
<td>508</td>
</tr>
<tr>
<td>8.7.4.9.3</td>
<td>Associating an XML Document Definition to a Source</td>
<td>512</td>
</tr>
<tr>
<td>8.7.4.10</td>
<td>Administration Tool - SharePoint Menu</td>
<td>513</td>
</tr>
<tr>
<td>8.7.4.10.1</td>
<td>What Is the Structure of SharePoint?</td>
<td>513</td>
</tr>
<tr>
<td>8.7.4.10.2</td>
<td>What Are SharePoint Reference Sets?</td>
<td>514</td>
</tr>
<tr>
<td>8.7.4.10.3</td>
<td>Adding a SharePoint Reference Set</td>
<td>514</td>
</tr>
<tr>
<td>8.7.4.10.4</td>
<td>Adding and Modifying SharePoint References</td>
<td>515</td>
</tr>
<tr>
<td>8.7.4.10.5</td>
<td>How CES Indexes SharePoint Items</td>
<td>517</td>
</tr>
<tr>
<td>8.7.4.10.6</td>
<td>Available Item Types</td>
<td>518</td>
</tr>
<tr>
<td>8.7.4.10.7</td>
<td>Available List Base Types</td>
<td>519</td>
</tr>
<tr>
<td>8.7.4.10.8</td>
<td>Adding New Properties to SharePoint References</td>
<td>519</td>
</tr>
<tr>
<td>8.7.4.10.9</td>
<td>What Is the Difference between Structured and Unstructured Information?</td>
<td>521</td>
</tr>
<tr>
<td>8.7.4.10.10</td>
<td>Indexing Structured Information in SharePoint Sources</td>
<td>521</td>
</tr>
<tr>
<td>8.7.4.10.11</td>
<td>Determining the Name of a SharePoint Metadata Tag</td>
<td>522</td>
</tr>
<tr>
<td>8.7.4.10.12</td>
<td>Indexing Unstructured Information in SharePoint Sources</td>
<td>522</td>
</tr>
<tr>
<td>8.7.4.11</td>
<td>Administration Tool - License Menu</td>
<td>522</td>
</tr>
<tr>
<td>8.7.4.11.1</td>
<td>About the Coveo License</td>
<td>523</td>
</tr>
<tr>
<td>8.7.4.11.2</td>
<td>Entering a New License Code</td>
<td>523</td>
</tr>
<tr>
<td>8.7.4.11.3</td>
<td>What Information Is Displayed in the License Page?</td>
<td>525</td>
</tr>
</tbody>
</table>
8.7.4.11.4 License Document Limit Notifications ......................................................... 528
8.7.4.12 Administration Tool - Alerts Menu ................................................................. 528
  8.7.4.12.1 Configuring Email Alerts ............................................................................. 528
8.7.4.13 Administration Tool - Pre-loading Menu ........................................................... 531
  8.7.4.13.1 Pre-Loading a .NET Search Page to Prevent Display Delays ....................... 531
8.7.4.14 Administration Tool - Advanced Menu ............................................................. 533
  8.7.4.14.1 Modifying Advanced CES Parameters ......................................................... 533
8.7.5 Administration Tool - Support Tab ....................................................................... 536
8.7.6 Opening the .NET Interface Editor ....................................................................... 537
8.7.7 Navigating in the .NET Interface Editor ............................................................... 538
8.7.8 .NET Interface Editor - Search Hubs Tab .............................................................. 539
  8.7.8.1 What Is a Search Hub? ...................................................................................... 540
  8.7.8.2 Creating a Search Hub With the .NET Interface Editor .................................... 540
  8.7.8.3 Deleting a Search Hub With the .NET Interface Editor .................................... 541
  8.7.8.4 Previewing a Search Hub in a Browser With the .NET Interface Editor ............... 542
  8.7.8.5 What Is a Search Interface? ............................................................................... 542
  8.7.8.6 Making Search Interfaces Available in a Search Hub With the .NET Interface Editor .... 543
  8.7.8.7 Adding Search Interfaces to a Search Hub With the .NET Interface Editor .......... 544
  8.7.8.8 Enabling Mini-Results in Search Interfaces With the .NET Interface Editor .......... 545
  8.7.8.9 Limiting the Quick View Size in Search Interfaces With the .NET Interface Editor .... 546
  8.7.8.10 Configuring a .NET Hub to Show a Drop-Down List for Overflowing Search Interface Links . 548
  8.7.8.11 Configuring the General Search Hub Parameters With the .NET Interface Editor .... 549
  8.7.8.12 Configuring the Culture of a Search Hub With the .NET Interface Editor .......... 550
8.7.9 .NET Interface Editor - Search Interfaces Tab .......................................................... 555
  8.7.9.1 What Are the .NET Search Interface Page Types? ............................................ 558
  8.7.9.2 Creating a Search Interface With the .NET Interface Editor .............................. 559
  8.7.9.3 .NET Interface Editor - Features Menu .............................................................. 561
    8.7.9.3.1 What Are Skins? ......................................................................................... 561
    8.7.9.3.2 Changing the Logo Appearing in a Search Interface With the .NET Interface Editor ...... 561
    8.7.9.3.3 Adding Related Results Display Templates With the .NET Interface Editor .......... 562
    8.7.9.3.4 Activating Search Interface Options With the .NET Interface Editor ............... 565
8.10.8.6.4 Predefined Text Analytics Normalizers  .................................................. 722
8.10.8.6.4.1 MetadataBlackLister ................................................................. 722
8.10.8.6.4.2 MetadataRegexBlacklister ......................................................... 722
8.10.8.6.4.3 MetadataFilter ................................................................. 722
8.10.8.6.4.4 MetadataNormalizer ............................................................... 723
8.10.8.6.5 Predefined Text Analytics Outputters ............................................... 724
8.10.8.6.5.1 CESITaggerOutputter ............................................................... 724
8.10.8.6.5.2 FSDumpMetadataPrinter ......................................................... 726
8.10.8.6.5.3 FSDumpResultProcessor ......................................................... 727
8.10.8.7 Predefined Text Analytics Job Plugins ............................................... 727
8.10.8.7.1 CreateTagField ................................................................. 727
8.10.8.7.2 ClearFieldJob ................................................................. 728
8.10.8.7.3 MasterFieldMoverJob ............................................................... 728
8.10.8.7.4 BlacklistJob ................................................................. 729
8.10.8.7.5 NormalizationJob ............................................................... 729
8.10.8.7.6 WhitelistBasicMatcherJob ....................................................... 730
8.10.8.7.7 WhitelistQueryMatcherJob ....................................................... 730
8.10.9 Clearing Text Analytics Tag Fields ...................................................... 731
8.10.10 Reprocessing All Documents with a Text Analytics Run ........................................... 732

9. Coveo Platform Connectors .................................................................. 734

9.1 What Does Deprecated Mean for a Coveo Connector? ................................. 739
9.1.1 Connector Deprecation ........................................................................ 739
9.1.2 Repository Version Support Deprecation ............................................ 740
9.2 Aha! Connector ....................................................................................... 740
9.2.1 Features ......................................................................................... 741
9.2.2 Limitation ......................................................................................... 741
9.2.3 Aha! Connector Deployment Overview ............................................ 742
9.2.4 Aha! Connector Requirements ......................................................... 742
9.2.5 Granting the Connector Access to Your Aha! Content ........................................... 742
9.2.6 Configuring and Indexing a Aha! Source ........................................... 744
9.3 Alfresco One Connector ......................................................................... 748
<table>
<thead>
<tr>
<th>SECTION</th>
<th>PAGE</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.6.6 Configuring an Atlassian Confluence V2 Security Provider</td>
<td>795</td>
</tr>
<tr>
<td>9.6.7 Configuring and Indexing an Atlassian Confluence V2 Source</td>
<td>797</td>
</tr>
<tr>
<td>9.6.8 Modifying Hidden Atlassian Confluence V2 Source Parameters</td>
<td>804</td>
</tr>
<tr>
<td>9.7 Atlassian Jira Software V2 Connector</td>
<td>806</td>
</tr>
<tr>
<td>9.7.1 Connector Features Summary</td>
<td>806</td>
</tr>
<tr>
<td>9.7.2 Features</td>
<td>807</td>
</tr>
<tr>
<td>9.7.3 Atlassian Jira Software V2 Connector Deployment Overview</td>
<td>808</td>
</tr>
<tr>
<td>9.7.4 Atlassian Jira V2 Connector Requirements</td>
<td>810</td>
</tr>
<tr>
<td>9.7.5 Creating a Jira Software Webhook</td>
<td>810</td>
</tr>
<tr>
<td>9.7.6 Installing the Coveo Plugin for Atlassian Jira Software</td>
<td>814</td>
</tr>
<tr>
<td>9.7.7 Configuring an Atlassian Jira Software V2 Security Provider</td>
<td>817</td>
</tr>
<tr>
<td>9.7.8 Configuring and Indexing an Atlassian Jira Software V2 Source</td>
<td>820</td>
</tr>
<tr>
<td>9.7.8.1 Modifying Hidden Atlassian Jira Software V2 Source Parameters</td>
<td>827</td>
</tr>
<tr>
<td>9.8 Basecamp Connector</td>
<td>829</td>
</tr>
<tr>
<td>9.8.1 Features</td>
<td>829</td>
</tr>
<tr>
<td>9.8.2 Limitations</td>
<td>830</td>
</tr>
<tr>
<td>9.8.3 Basecamp Connector Deployment Overview</td>
<td>830</td>
</tr>
<tr>
<td>9.8.4 Basecamp Connector Requirements</td>
<td>831</td>
</tr>
<tr>
<td>9.8.5 Authorizing the Coveo Connector to Access Your Basecamp Content</td>
<td>831</td>
</tr>
<tr>
<td>9.8.6 Configuring and Indexing a Basecamp Source</td>
<td>835</td>
</tr>
<tr>
<td>9.8.6.1 Modifying Hidden Basecamp Source Parameters</td>
<td>840</td>
</tr>
<tr>
<td>9.9 Box Connector</td>
<td>841</td>
</tr>
<tr>
<td>9.9.1 Connector Features Summary</td>
<td>841</td>
</tr>
<tr>
<td>9.9.2 Features</td>
<td>841</td>
</tr>
<tr>
<td>9.9.3 Limitations</td>
<td>842</td>
</tr>
<tr>
<td>9.9.4 Box Connector Deployment Overview</td>
<td>843</td>
</tr>
<tr>
<td>9.9.5 Box Connector Requirements</td>
<td>844</td>
</tr>
<tr>
<td>9.9.6 Authorizing the Coveo Connector to Access the Box of Your Managed Users</td>
<td>845</td>
</tr>
<tr>
<td>9.9.7 Configuring a Box Security Provider</td>
<td>847</td>
</tr>
<tr>
<td>9.9.8 Configuring and Indexing a Box Source</td>
<td>849</td>
</tr>
<tr>
<td>9.9.8.1 Modifying Hidden Box Source Parameters</td>
<td>854</td>
</tr>
</tbody>
</table>
9.15.3 Planning Your File Connector Collections and Sources .......................................... 940
9.15.4 Setting up a File System Crawling Account .......................................................... 942
9.15.5 Configuring and Indexing a File Connector Source .............................................. 942
  9.15.5.1 Modifying Hidden File Connector Source Parameters .................................... 948
9.15.6 Mail Archive Indexing with the File Connector ...................................................... 949
  9.15.6.1 About Permissions ........................................................................................... 950
  9.15.6.2 Live Monitoring Limitation ............................................................................. 950
  9.15.6.3 About the Mail Archives Modified Date Attribute ........................................... 951
  9.15.6.4 File Connector Mail Archive Indexing Deployment Overview .......................... 951
  9.15.6.5 Installing the Microsoft MAPI Component for Mail Archive Indexing .............. 951
  9.15.6.6 Setting up a Document Type for Mail Archive Indexing ................................. 958
  9.15.6.7 Creating a Mail Archive Mapping File ............................................................... 959
  9.15.6.7.1 Mail archive mapping file format .............................................................. 959
  9.15.7 Troubleshooting File Connector Issues ............................................................... 961

9.16 Gmail for Work Connector ....................................................................................... 963
  9.16.1 Connector Features Summary ............................................................................. 964
  9.16.2 Features ............................................................................................................ 964
  9.16.3 Gmail for Work Connector Deployment Overview ........................................... 965
  9.16.4 Gmail for Work Connector Requirements .......................................................... 966
  9.16.5 Setting Google Permissions Gmail for Work Connector ..................................... 967
    9.16.5.1 Authorizing the Coveo Connector to Access Your Users Gmail Mailboxes .... 967
    9.16.5.2 Authorizing the Coveo Connector to Access Your Google Apps for Work .... 971
  9.16.6 Configuring and Indexing a Gmail for Work Source ......................................... 973
    9.16.6.1 Modifying Hidden Gmail for Work Source Parameters .............................. 978

9.17 Google Drive for Work Compact Connector ............................................................. 979
  9.17.1 Connector Features Summary ............................................................................. 979
  9.17.2 Features ........................................................................................................... 980
  9.17.3 Google Drive for Work Compact Connector Deployment Overview ................... 981
  9.17.4 Google Drive for Work Compact Connector Requirements .................................. 982
  9.17.5 Setting Google Permissions (Google Drive for Work) ......................................... 983
    9.17.5.1 Authorizing the Coveo Connector to Access Your Google Drive ................. 983

www.coveo.com
9.22.9 Troubleshooting Jive 5/SBS/Clearspace Connector Issues ........................................... 1102
9.22.9.1 Group Permissions ................................................................. 1102
9.22.9.2 Incremental Refresh ............................................................... 1103
9.22.9.3 Secure Addresses ................................................................. 1103
9.22.9.4 Error during Refresh or Rebuild ................................................ 1103
9.23 Liferay Connector ......................................................................... 1104
9.23.1 Features .................................................................................. 1104
9.23.2 Limitations .............................................................................. 1105
9.23.3 Feature History ....................................................................... 1105
9.23.4 Liferay Connector Deployment Overview ...................................... 1105
9.23.5 Liferay Connector Requirements .................................................. 1107
9.23.6 About the Coveo Liferay Portlet Plugin Deployment ....................... 1108
  9.23.6.1 Deploying the Coveo Liferay Portlet Plug-in for Liferay 6.0 .................. 1108
  9.23.6.2 Deploying the Coveo Liferay Portlet Plug-in for Liferay 6.1 .................. 1111
9.23.7 Setting up a Liferay Crawling Account ........................................... 1114
9.23.8 CES Configuration for the Liferay Connector ................................... 1116
  9.23.8.1 Configuring a Liferay Security Provider ....................................... 1116
  9.23.8.2 Configuring and Indexing a Liferay Source ................................. 1118
  9.23.8.3 About the Liferay Connector Mapping File ................................... 1123
  9.23.8.4 Customizing the Liferay Connector Mapping File ......................... 1124
  9.23.8.5 Modifying Hidden Liferay Source Parameters ............................ 1125
9.24 Lithium Connector ......................................................................... 1127
  9.24.1 Connector Features Summary .................................................... 1127
  9.24.2 Features ................................................................................. 1128
  9.24.3 Lithium Connector Deployment Overview ...................................... 1129
  9.24.4 Configuring and Indexing a Lithium Source .................................... 1130
  9.24.5 Modifying Hidden Lithium Source Parameters ............................. 1138
9.25 Microsoft Active Directory Connector ............................................. 1141
  9.25.1 Configuring an Active Directory Security Provider ........................... 1141
  9.25.2 Configuring and Indexing an Active Directory Source ...................... 1143
9.26 Microsoft Dynamics CRM Connector ............................................... 1148
9.26.1 Limitations .............................................................................................................. 1149
9.26.2 Microsoft Dynamics CRM Connector Deployment Overview .............................. 1150
9.26.3 Microsoft Dynamics CRM Connector Requirements .............................................. 1151
9.26.4 Enabling Auditing of Your Microsoft Dynamics CRM Entities ............................ 1152
9.26.5 Microsoft Dynamics CRM Events Update Requirements ....................................... 1153
9.26.6 Setting Up a Microsoft Dynamics CRM Full Read Account .................................. 1155
9.26.7 Using the Microsoft Dynamics CRM Connector Configuration Generator Tool .......... 1159
9.26.8 Configuring a Microsoft Dynamics CRM Security Provider .................................. 1163
9.26.9 Configuring and Indexing a Microsoft Dynamics CRM Source ............................ 1165
  9.26.9.1 Modifying Hidden Microsoft Dynamics CRM Source Parameters ....................... 1171
9.26.10 Troubleshooting Microsoft Dynamics CRM Connector Issues ............................ 1173

9.27 Microsoft Exchange Connector .................................................................................. 1173
  9.27.1 Connector Features Summary ................................................................................ 1173
  9.27.2 Features .............................................................................................................. 1173
  9.27.3 Microsoft Exchange Connector Deployment Overview ........................................ 1175
  9.27.4 Microsoft Exchange Connector Requirements .................................................... 1178
  9.27.5 Microsoft Exchange Online Source Quick Setups ............................................... 1178
    9.27.5.1 Microsoft Exchange Online With Azure AD Users (Cloud-Based or Synced/Federated) Source Quick Setup ............................................................................. 1179
    9.27.5.2 Microsoft Exchange Online With Federated Users Source Quick Setup .............. 1181
  9.27.6 Microsoft Exchange Configuration for the Connector ............................................ 1183
    9.27.6.1 Creating a Microsoft Exchange Crawling Account ........................................ 1183
      9.27.6.1.1 Setting up a Full Read Microsoft Exchange Account .................................. 1185
    9.27.6.2 Authorizing the Coveo Connector to Access the Exchange Online Mailboxes of Your Azure AD Users ......................................................................................... 1186
    9.27.6.3 Configuring the Throttling Policy for the Microsoft Exchange Account ............... 1190
    9.27.6.4 Preventing Microsoft Exchange Public Folder Crawling Issues ....................... 1192
    9.27.6.5 Enabling Impersonation in Microsoft Exchange Online ................................... 1193
  9.27.7 CES Configuration for the Microsoft Exchange Connector .................................... 1194
    9.27.7.1 Configuring a Microsoft Exchange Security Provider ..................................... 1194
    9.27.7.2 Configuring and Indexing a Microsoft Exchange Source for an On-Premises Deployment .............................................................. 1197
      9.27.7.2.1 Choosing to Connect to Microsoft Exchange Using Web Services or WebDAV 1204
9.27.7.2.2 Fine-Tuning the Exchange Callback Service .................................................. 1204
9.27.7.3 Configuring and Indexing Microsoft Exchange Sources for a Hybrid Deployment .......... 1207
9.27.7.4 Configuring and Indexing Microsoft Exchange Sources for an Online Deployment .......... 1215
9.27.7.5 Modifying Hidden Microsoft Exchange Source Parameters ........................................ 1222
9.27.7.6 What Are LDAP Searches? ................................................................................. 1230

9.28 Microsoft Office 365 Support Information .................................................................. 1231
9.29 Microsoft OneDrive for Business Connector ............................................................... 1231
  9.29.1 Microsoft OneDrive for Business Connector Deployment Overview ................................ 1232
  9.29.2 Configuring and Indexing a Microsoft OneDrive for Business Source .......................... 1235
  9.29.2.1 Modifying Hidden Microsoft OneDrive for Business Source Parameters ................. 1240
    9.29.2.1.1 ADFS Related Parameters ............................................................................. 1240
    9.29.2.1.2 Other Parameters ....................................................................................... 1241

9.30 Microsoft SharePoint Connector ............................................................................... 1243
  9.30.1 Comparison With the Legacy Connector ................................................................. 1243
  9.30.2 Connector Features Summary .............................................................................. 1244
  9.30.3 Features .............................................................................................................. 1244
  9.30.4 Microsoft SharePoint Source Quick Setsups .......................................................... 1247
    9.30.4.1 SharePoint 2016/2013/2010 On-Premises (Windows Classic) [AD] Source Quick Setup ... 1247
    9.30.4.2 SharePoint 2016/2013/2010 On-Premises (Windows Under Claims) [Claims] Source Quick Setup ................................................................................................................ 1250
    9.30.4.3 SharePoint 2016/2013/2010 On-Premises (ADFS Under Claims) [Claims] Source Quick Setup ...................................................................................................................... 1252
    9.30.4.4 SharePoint 2016/2013/2010 On-Premises (Federated - Okta) Source Quick Setup .......... 1256
    9.30.4.5 SharePoint Online (Native) [Claims] Source Quick Setup ........................................ 1259
    9.30.4.6 SharePoint Online (ADFS SSO) [Claims] Source Quick Setup ................................. 1261
    9.30.4.7 SharePoint Online (Okta SSO) [Claims] Source Quick Setup ...................................... 1265
    9.30.4.8 SharePoint Online (Federated - Okta) [Email] Source Quick Setup ............................. 1269
    9.30.4.9 SharePoint Online (Federated - ADFS) [Email] Source Quick Setup ............................ 1273
    9.30.4.10 SharePoint Online (Native) [Email] Source Quick Setup ......................................... 1276

9.30.5 Microsoft SharePoint Connector Deployment Overview ........................................... 1279
9.30.6 Listing User Profiles With a SharePoint Search Service Application ......................... 1283
9.30.7 Creating a SharePoint Security Provider .................................................................... 1284
<table>
<thead>
<tr>
<th>Section</th>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.32.8</td>
<td>SharePoint Source Refresh Troubleshooting for the Legacy Connector</td>
<td>1357</td>
</tr>
<tr>
<td>9.33</td>
<td>OpenText Content Server Connector</td>
<td>1358</td>
</tr>
<tr>
<td>9.33.1</td>
<td>OpenText Content Server Connector Deployment Overview</td>
<td>1360</td>
</tr>
<tr>
<td>9.33.2</td>
<td>OpenText Content Server Connector Requirements</td>
<td>1362</td>
</tr>
<tr>
<td>9.33.3</td>
<td>Enabling the OpenText Content Server Web Services</td>
<td>1362</td>
</tr>
<tr>
<td>9.33.3.1</td>
<td>Connecting the OTCS Web Services</td>
<td>1362</td>
</tr>
<tr>
<td>9.33.3.2</td>
<td>Setting IIS Permissions</td>
<td>1364</td>
</tr>
<tr>
<td>9.33.3.3</td>
<td>Enabling WCF Services</td>
<td>1365</td>
</tr>
<tr>
<td>9.33.4</td>
<td>Setting Up an OpenText Content Server Crawling Account</td>
<td>1365</td>
</tr>
<tr>
<td>9.33.5</td>
<td>Configuring an OpenText Content Server Security Provider</td>
<td>1367</td>
</tr>
<tr>
<td>9.33.6</td>
<td>Configuring and Indexing an OpenText Content Server Source</td>
<td>1370</td>
</tr>
<tr>
<td>9.33.6.1</td>
<td>Creating an OpenText Content Server Connector Mapping File</td>
<td>1376</td>
</tr>
<tr>
<td>9.33.6.2</td>
<td>Modifying Hidden OpenText Content Server Source Parameters</td>
<td>1377</td>
</tr>
<tr>
<td>9.34</td>
<td>Oracle Knowledge Connector</td>
<td>1381</td>
</tr>
<tr>
<td>9.34.1</td>
<td>Features</td>
<td>1381</td>
</tr>
<tr>
<td>9.34.2</td>
<td>Limitation</td>
<td>1381</td>
</tr>
<tr>
<td>9.34.3</td>
<td>Oracle Knowledge Connector Deployment Overview</td>
<td>1382</td>
</tr>
<tr>
<td>9.34.4</td>
<td>Oracle Knowledge Connector Requirements</td>
<td>1383</td>
</tr>
<tr>
<td>9.34.5</td>
<td>Configuring an Oracle Knowledge Security Provider</td>
<td>1384</td>
</tr>
<tr>
<td>9.34.6</td>
<td>Configuring and Indexing an Oracle Knowledge Source</td>
<td>1386</td>
</tr>
<tr>
<td>9.34.6.1</td>
<td>Modifying Hidden Oracle Knowledge Source Parameters</td>
<td>1392</td>
</tr>
<tr>
<td>9.34.7</td>
<td>Troubleshooting Oracle Knowledge Connector Issues</td>
<td>1393</td>
</tr>
<tr>
<td>9.35</td>
<td>Oracle UCM Connector</td>
<td>1394</td>
</tr>
<tr>
<td>9.35.1</td>
<td>Features</td>
<td>1394</td>
</tr>
<tr>
<td>9.35.2</td>
<td>Oracle UCM Connector Deployment Overview</td>
<td>1395</td>
</tr>
<tr>
<td>9.35.3</td>
<td>Oracle UCM Connector Requirements</td>
<td>1396</td>
</tr>
<tr>
<td>9.35.4</td>
<td>Configuring Oracle UCM to Allow Access from the Coveo Server</td>
<td>1396</td>
</tr>
<tr>
<td>9.35.5</td>
<td>Creating an Oracle UCM Crawling Account</td>
<td>1399</td>
</tr>
<tr>
<td>9.35.6</td>
<td>Configuring an Oracle UCM Security Provider</td>
<td>1403</td>
</tr>
<tr>
<td>9.35.7</td>
<td>Configuring and Indexing an Oracle UCM Source</td>
<td>1407</td>
</tr>
<tr>
<td>9.35.8</td>
<td>About the Oracle UCM Mapping File</td>
<td>1412</td>
</tr>
</tbody>
</table>
9.38.8.7 Salesforce ObjectsToGet Configuration File Example for CRM Content .......................... 1488
9.38.8.8 Salesforce ObjectsToGet Configuration File Example for Chatter Objects .......................... 1491
9.38.8.9 Salesforce Connector Configuration Recipes ................................................................. 1494
  9.38.8.9.1 Indexing all Knowledge Base Versions and States ...................................................... 1494
  9.38.8.9.2 Excluding Archived Knowledge Base Articles .......................................................... 1496
  9.38.8.9.3 Indexing Knowledge Base Attachments ........................................................................ 1497
  9.38.8.9.4 Fetching Records With Parent Relationships That Must Be Incrementally Updated ... 1498
  9.38.8.9.5 Fetching Child Relationship to Use for Folding ............................................................. 1499
  9.38.8.9.6 Fetch Child Relationship to Use to Increase or Reduce Results From Queries ............. 1500
  9.38.8.9.7 Minimizing API Calls and Object Description Prefetching ............................................ 1501
  9.38.8.9.8 Fetching Records Faster Using the Turbo Mode Runner ................................................ 1501
  9.38.8.9.9 Reducing the Metadata Package Size by Scoping Parents of ContentVersion and Attachment Objects ................................................................................................................................. 1503
  9.38.8.9.10 Choosing the Optimal Record Modification Date Field .............................................. 1503
  9.38.8.9.11 Removing Leading Zeroes of a Field ........................................................................... 1504
  9.38.8.9.12 Using the Currency Field Converter .......................................................................... 1504
  9.38.8.9.13 Using the FiscalYearResolver .................................................................................... 1504
  9.38.8.9.14 Fixing the Feed Tracking Error .................................................................................... 1504
  9.38.8.9.15 Indexing More Than the Built-in FeedItem Types ....................................................... 1505
9.38.9 Creating a Salesforce Mapping File ..................................................................................... 1505
  9.38.9.1 Salesforce Mapping File Example for Standard Objects .................................................. 1507
  9.38.9.2 Salesforce Mapping File Example for Knowledge Base .................................................. 1525
  9.38.9.3 Salesforce Mapping File Example for CRM Content ..................................................... 1529
  9.38.9.4 Salesforce Mapping File Example for Chatter Objects ................................................... 1532
9.38.10 Configuring a Salesforce Security Provider ......................................................................... 1534
  9.38.11 Configuring and Indexing a Salesforce Source ................................................................. 1536
    9.38.11.1 Modifying Hidden Salesforce Source Parameters ..................................................... 1543
9.38.12 Troubleshooting Salesforce Connector Issues ................................................................. 1543
  9.38.12.1 API Security Token Required ....................................................................................... 1546
  9.38.12.2 Expired Access/Refresh Token .................................................................................... 1546
  9.38.12.3 Missing ionic.zip File .................................................................................................... 1546
<table>
<thead>
<tr>
<th>Section</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.39 Salesforce Legacy Connector</td>
</tr>
<tr>
<td>9.39.1 Features</td>
</tr>
<tr>
<td>9.39.2 Determining If Sources Use the Salesforce Legacy Connector</td>
</tr>
<tr>
<td>9.39.3 Salesforce Legacy Connector Deployment Overview</td>
</tr>
<tr>
<td>9.39.4 Salesforce Legacy Connector Requirements</td>
</tr>
<tr>
<td>9.39.5 About the Default Salesforce Mapping File for the Legacy Connector</td>
</tr>
<tr>
<td>9.39.5.1 Managing Permissions</td>
</tr>
<tr>
<td>9.39.5.2 Default Mapping File Content</td>
</tr>
<tr>
<td>9.39.6 Creating and Using a Custom Salesforce Mapping File for the Legacy Connector</td>
</tr>
<tr>
<td>9.39.6.1 Mapping file structure</td>
</tr>
<tr>
<td>9.39.6.2 Mapping child nodes</td>
</tr>
<tr>
<td>9.39.6.3 Mapping local expressions</td>
</tr>
<tr>
<td>9.39.6.4 Mapping foreign expressions</td>
</tr>
<tr>
<td>9.39.6.5 Using external resolvers</td>
</tr>
<tr>
<td>9.39.7 Configuring a Salesforce Security Provider for the Legacy Connector</td>
</tr>
<tr>
<td>9.39.8 Configuring and Indexing a Salesforce Source for the Legacy Connector</td>
</tr>
<tr>
<td>9.39.9 Modifying Hidden Salesforce Source Parameters for the Legacy Connector</td>
</tr>
<tr>
<td>9.40 Sitemap Connector</td>
</tr>
<tr>
<td>9.40.1 Connector Features Summary</td>
</tr>
<tr>
<td>9.40.2 Features</td>
</tr>
<tr>
<td>9.40.3 Sitemap Connector Deployment Overview</td>
</tr>
<tr>
<td>9.40.4 Sitemap Connector Requirements</td>
</tr>
<tr>
<td>9.40.5 Configuring and Indexing a Sitemap Source</td>
</tr>
<tr>
<td>9.40.5.1 Modifying Hidden Sitemap Source Parameters</td>
</tr>
<tr>
<td>9.40.6 Adding and Indexing Custom Metadata in an XML Sitemap</td>
</tr>
<tr>
<td>9.41 Symantec Enterprise Vault Connector</td>
</tr>
<tr>
<td>9.41.1 Features</td>
</tr>
<tr>
<td>9.41.2 Feature history</td>
</tr>
<tr>
<td>9.41.3 Symantec Enterprise Vault Connector Deployment Overview</td>
</tr>
<tr>
<td>9.41.4 Symantec Enterprise Vault Connector Requirements</td>
</tr>
<tr>
<td>9.41.5 Enabling Symantec Enterprise Vault Services</td>
</tr>
</tbody>
</table>
9.41.6 Impersonating a Symantec Enterprise Vault User ............................................ 1590
9.41.7 Configuring and Indexing a Symantec Enterprise Vault Source ............................................ 1590
9.41.8 Modifying Hidden Symantec Enterprise Vault Source Parameters ............................................ 1595
9.42 Twitter v2 Connector ...................................................... 1
9.42.1 Features ................................................................. 1
9.42.2 Limitations ............................................................. 2
9.42.3 Twitter v2 Connector Deployment Overview .................................................. 2
9.42.4 Twitter v2 Connector Requirements .................................................. 2
9.42.5 Obtaining the Twitter API and Access Token .................................................. 3
9.42.6 Configuring and Indexing a Twitter v2 Source .................................................. 5
9.42.6.1 Modifying Hidden Twitter v2 Source Parameters .................................................. 12
9.43 Web Pages Connector .................................................. 13
9.43.1 Configuring and Indexing a Web Pages Source .................................................. 14
9.44 Yammer Connector ................................................... 20
9.44.1 Features ................................................................. 20
9.44.2 Yammer Connector Deployment Overview .................................................. 21
9.44.3 Yammer Connector Requirements .................................................. 22
9.44.4 Authorizing the Coveo Connector to Access Your Yammer Network .................................................. 22
9.44.5 Configuring a Yammer Security Provider .................................................. 24
9.44.6 Configuring and Indexing a Yammer Source .................................................. 26
9.45 YouTube Connector .................................................. 30
9.45.1 Connector Features Summary .................................................. 30
9.45.2 Features ................................................................. 31
9.45.3 Limitation ............................................................. 31
9.45.4 YouTube Connector Deployment Overview .................................................. 32
9.45.5 YouTube Connector Requirements .................................................. 32
9.45.6 Allowing the Coveo Connector Access to YouTube Data .................................................. 33
9.45.7 Configuring and Indexing a YouTube Source .................................................. 36
9.45.7.1 Modifying Hidden YouTube Source Parameters .................................................. 42
9.46 Zendesk Connector ................................................... 43
9.46.1 Features ................................................................. 43
11.4.3.1 Microsoft SQL Server 2008 and 2005 .................................................. 94
11.4.3.2 Microsoft SQL Server 2000 ................................................................. 95
11.4.4 Adding the Database Owner Role for Microsoft SQL Server .................. 96
11.4.4.1 Microsoft SQL Server 2008/2005 ......................................................... 96
11.4.4.2 Microsoft SQL Server 2000 ................................................................. 98
11.5 Microsoft SharePoint .............................................................................. 99
11.5.1 Adding the Full Read Policy to All SharePoint Farm Web Applications .......... 99
11.5.1.1 Microsoft SharePoint 2013 or 2010 ....................................................... 99
11.5.1.2 Microsoft SharePoint 2007 ................................................................. 100
11.5.2 Adding the SharePoint Website Read Permission .................................... 101
11.5.2.1 Microsoft SharePoint 2013 or 2010 ....................................................... 101
11.5.2.2 Microsoft SharePoint 2007 ................................................................. 102
11.5.3 Adding the Retrieve People Data for Search Crawlers Permission to the User Profile Service Application .......................................................... 103
11.5.4 Adding the Manage User Profiles Permission in Shared Service Rights ........ 105
11.5.5 Adding the Crawling Account to the SharePoint Farm Administrators Group .......... 105
11.5.5.1 Microsoft SharePoint 2013 ................................................................. 106
11.5.5.2 Microsoft SharePoint 2010 ................................................................. 107
11.5.5.3 Microsoft SharePoint 2007 ................................................................. 108
11.5.6 Finding the Assembly Type of a SharePoint Web Part ............................. 109
11.5.7 Finding the Enabled Claims Authentication Type for a SharePoint Web Application .......... 110
11.5.8 Finding and Enabling the ADFS Service Endpoint URL Path .................. 110
11.5.9 Finding Your Office 365 Native Domain Name ......................................... 111
11.5.10 Finding the Relying Party Trust Identifier for a SharePoint Web Application .......... 111
11.5.11 Finding the Relying Party Trust Identifier for a SharePoint ADFS server ........ 112
11.5.12 Granting the Site Collection Administrator Permission in SharePoint Online .......... 112
11.5.13 Adding the Personal Sites Collections Owner Permissions for SharePoint Online .......... 113
11.6 Microsoft Windows Server ..................................................................... 117
11.6.1 Adding the Crawling Account to the SharePoint Server Local Administrators Group .......... 118
11.7 Changing the RabbitMQ Administrator Password ......................................... 118
12. CES Performance .................................................................................... 121
<table>
<thead>
<tr>
<th>Chapter</th>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.1</td>
<td>Limiting the Size of the Coveo index</td>
<td>121</td>
</tr>
<tr>
<td>12.2</td>
<td>Speeding up CES</td>
<td>122</td>
</tr>
<tr>
<td>12.3</td>
<td>Configuring the Index to Ignore Stop Words in Queries</td>
<td>124</td>
</tr>
<tr>
<td>13.1</td>
<td>Coveo Platform Troubleshooting Guide</td>
<td>126</td>
</tr>
<tr>
<td>13.1.1</td>
<td>CES Service</td>
<td>126</td>
</tr>
<tr>
<td>13.2</td>
<td>Crawling</td>
<td>127</td>
</tr>
<tr>
<td>13.3</td>
<td>Performance</td>
<td>128</td>
</tr>
<tr>
<td>13.4</td>
<td>Search Interface</td>
<td>129</td>
</tr>
<tr>
<td>13.5</td>
<td>About the Coveo SystemStatus Tool</td>
<td>129</td>
</tr>
<tr>
<td>13.5.1</td>
<td>Coveo SystemStatus Tool Requirements</td>
<td>129</td>
</tr>
<tr>
<td>13.5.2</td>
<td>Files Gathered by the Coveo SystemStatus Tool</td>
<td>130</td>
</tr>
<tr>
<td>13.5.3</td>
<td>Using the Coveo SystemStatus Tool</td>
<td>131</td>
</tr>
<tr>
<td>13.5.3.1</td>
<td>Downloading and Installing</td>
<td>131</td>
</tr>
<tr>
<td>13.5.3.2</td>
<td>Gathering System Information</td>
<td>132</td>
</tr>
<tr>
<td>13.6</td>
<td>Getting Debug Information from a .NET Search Interface</td>
<td>135</td>
</tr>
<tr>
<td>13.7</td>
<td>Gathering Windows Server Performance Monitor Information</td>
<td>135</td>
</tr>
<tr>
<td>13.8</td>
<td>Using Transaction Trace Logging</td>
<td>138</td>
</tr>
<tr>
<td>13.9</td>
<td>Using Query Profiling</td>
<td>138</td>
</tr>
<tr>
<td>13.10</td>
<td>Logging Information With log4net</td>
<td>139</td>
</tr>
<tr>
<td>13.10.1</td>
<td>How log4net Works</td>
<td>139</td>
</tr>
<tr>
<td>13.11</td>
<td>Why Are Some Documents Not Returned by the Search Engine?</td>
<td>142</td>
</tr>
<tr>
<td>13.12</td>
<td>Why does the Initial .NET Search Page Take Much Longer to Appear?</td>
<td>145</td>
</tr>
<tr>
<td>13.13</td>
<td>Cannot Connect to the Instance Default</td>
<td>146</td>
</tr>
<tr>
<td>13.14</td>
<td>Access Denied Message When Opening a Result</td>
<td>147</td>
</tr>
<tr>
<td>13.15</td>
<td>Certificate Error</td>
<td>147</td>
</tr>
<tr>
<td>13.16</td>
<td>Cannot Find SharePoint Documents</td>
<td>147</td>
</tr>
<tr>
<td>13.17</td>
<td>Resolving Slow Search Interface Loading in Sitecore</td>
<td>148</td>
</tr>
<tr>
<td>13.18</td>
<td>Security Provider Not Properly Configured</td>
<td>148</td>
</tr>
<tr>
<td>13.19</td>
<td>Time Zone Error</td>
<td>150</td>
</tr>
<tr>
<td>13.20</td>
<td>Unsupported Back-End Version for a .NET Search Interface</td>
<td>151</td>
</tr>
<tr>
<td>13.21</td>
<td>SharePoint Error - Number of Lookup Columns</td>
<td>151</td>
</tr>
</tbody>
</table>
1. Introduction

The Coveo Platform is an information consolidation system composed of front-end and back-end services. On the back-end, the Coveo Enterprise Search (CES) service builds and maintains a unified index of contents from several systems and repositories within your organization. The Coveo administrator uses the Administration Tool to perform CES service related tasks. The CES service returns query results received from search interfaces.

On the front-end, the search interfaces and other specialized dashboards allow end-users to efficiently find information. The web-based search interfaces are made available through Microsoft IIS. The Coveo administrator uses the Interface Editor to configure the search interfaces.

Depending on the size of your Coveo implementation, both front-end and back-end Coveo services can reside on one server or can be deployed on several servers (see "Coveo Scalability Model" on page 14 and "Deployment" on page 12).

This guide contains information to help the Coveo administrator install, deploy, configure, manage, optimize, and migrate the Coveo Platform.
2. Coveo Platform Hardware and Software Requirements

This topic presents the hardware, software, and operating system specs for the server on which you install Coveo Enterprise Search (CES) for various index size ranges that one Coveo instance can manage. The system specifications apply to back-end Coveo Master and Mirror servers.

Notes:

- Operate CES on a dedicated server. When other processes are running in parallel or when the query activity reaches peaks and becomes mission-critical, a server meeting the specified requirements may not be sufficient.
- Coveo products work best on physical machines, but also support virtual environments such as VMware (ESX), Microsoft Hyper-V, Amazon Web Services (AWS), Microsoft Azure.
- Consider distributing the index over more than one Coveo instance when the number of documents to index exceeds the maximum index size presented in this topic (see Coveo Scalability Model).
- Contact Coveo Support for assistance to select the best Coveo configuration for your environment.

2.1 Index of up to 5 Million Documents (Minimum Requirements)

<table>
<thead>
<tr>
<th>Component</th>
<th>Minimum Requirement</th>
</tr>
</thead>
<tbody>
<tr>
<td>Operating System</td>
<td>Windows Server</td>
</tr>
<tr>
<td>CPU - Processors</td>
<td>4 Core (1×4), 2.0 GHz or higher</td>
</tr>
<tr>
<td>RAM - Memory</td>
<td>16 GB</td>
</tr>
<tr>
<td>Disk - OS and Program Files</td>
<td>1 x 150 GB SATA 7.2/10 K RPM</td>
</tr>
<tr>
<td>Disk - Index (1 slice)</td>
<td>1 x 300 GB SATA 7.2/10 K RPM</td>
</tr>
<tr>
<td>Disk - Near Real-Time Indexing (optional)</td>
<td>1 x 150 GB SSD or SATA 7.2/10 K RPM</td>
</tr>
</tbody>
</table>

Important: Ensure that your environment meets the above minimum requirements and follows recommendations below before contacting Coveo Support to get help for a performance issue.

2.2 Index From 5 to 20 Million Documents

<table>
<thead>
<tr>
<th>Component</th>
<th>Recommendation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Operating System</td>
<td>Windows Server</td>
</tr>
<tr>
<td>CPU - Processors</td>
<td>8 Core (1×8), 2.0 GHz or higher</td>
</tr>
</tbody>
</table>

www.coveo.com
<table>
<thead>
<tr>
<th>Component</th>
<th>Recommendation</th>
</tr>
</thead>
<tbody>
<tr>
<td>RAM - Memory</td>
<td>32 GB</td>
</tr>
<tr>
<td>Disks - OS and Program Files</td>
<td>2 x 150 GB SAS 10/15 K RPM, RAID 1</td>
</tr>
<tr>
<td>Disks - Index (1 slice)</td>
<td>2 x 600 GB SAS 10/15 K RPM, RAID 1</td>
</tr>
<tr>
<td>Disks - Other CES Files</td>
<td>2 x 300 GB SAS 10/15 K RPM, RAID 1</td>
</tr>
<tr>
<td>Disk - Near Real-Time Indexing (optional)</td>
<td>2 x 300 GB SSD or SATA 10 K RPM, RAID 1</td>
</tr>
</tbody>
</table>

2.3 Index From 20 to 40 Million Documents

<table>
<thead>
<tr>
<th>Component</th>
<th>Recommendation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Operating System</td>
<td>Windows Server</td>
</tr>
<tr>
<td>CPU - Processors</td>
<td>16 Core (2×8) to 24 Core (2×12), 2.4 GHz or higher</td>
</tr>
<tr>
<td>RAM - Memory</td>
<td>64 GB</td>
</tr>
<tr>
<td>Disks - OS and Program Files</td>
<td>2 x 150 GB SAS 10/15 K RPM, RAID 1</td>
</tr>
<tr>
<td>Disks - Index (1 slice)</td>
<td>4 x 600 GB SAS 10/15 K RPM, RAID 10</td>
</tr>
<tr>
<td>Disks - Other CES Files</td>
<td>2 x 600 GB SAS 10/15 K RPM, RAID 1</td>
</tr>
<tr>
<td>Disk - Near Real-Time Indexing (optional)</td>
<td>2 x 300 GB SSD or SATA 10 K RPM, RAID 1</td>
</tr>
</tbody>
</table>

2.4 Index From 40 to 80 Million Documents

<table>
<thead>
<tr>
<th>Component</th>
<th>Recommendation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Operating System</td>
<td>Windows Server</td>
</tr>
<tr>
<td>CPU - Processors</td>
<td>24 Core (2×12) to 32 Core (4×8), 2.4 GHz or higher</td>
</tr>
<tr>
<td>RAM - Memory</td>
<td>128 GB</td>
</tr>
<tr>
<td>Disks - OS and Program Files</td>
<td>2 x 150 GB SAS 10/15 K RPM, RAID 1</td>
</tr>
<tr>
<td>Disks - Index (slice 1)</td>
<td>4 x 600 GB SAS 10/15 K RPM, RAID 10</td>
</tr>
<tr>
<td>Disks - Index (slice 2)</td>
<td>4 x 600 GB SAS 10/15 K RPM, RAID 10</td>
</tr>
<tr>
<td>Disks - Other CES Files</td>
<td>2 x 600 GB SAS 10/15 K RPM, RAID 1</td>
</tr>
<tr>
<td>Disk - Near Real-Time Indexing (optional)</td>
<td>2 x 300 GB SSD or SATA 10 K RPM, RAID 1</td>
</tr>
</tbody>
</table>
Important: No server should hold more than 80 million documents. When a server exceeds this limit, it is recommended to split the content logically and have search interfaces built around GDI, aggregating results from multiple indexes (see Coveo Scalability Model). Splitting any other way and have all queries go against all indexes would reduce performance.

Example: Your server holds 120 million documents of which 70 million are emails. The best way to split the content would be to have the archived emails on a server, the live emails on another, and other types of content on a third server. That way, when one of your users is searching for emails, their queries go in the index with the live emails. You could also enable the option to add archived emails (disabled by default) in the mix, and have another search interface for your other content.

2.5 Operating System Compatibility

The servers on which CES or Coveo .NET Front-End run must use one of the following OS:

- Windows Server 2016
  - CES 7.0.8996+ (June 2017) Coveo .NET Front-End 12.0.1883+ (June 2017)
- Windows Server 2012 R2 (with IIS 8) x64
  - CES 7.0.6196+ (November 2013) Coveo .NET Front-End 12.0.446+ (November 2013)
- Windows Server 2012 (with IIS 8) x64
  - CES 7.0.4897+ (December 2012) Coveo .NET Front-End 12.0.61+ (December 2012)
- Windows Server 2008 R2 (with IIS 7) x64
- Windows Server 2008 (with IIS 7)

Important: The x64 Windows OS version is required for indexes with more than 500 K documents.

Notes: CES can operate on non-server versions of Windows operating systems. However, for production purposes, Coveo only supports and recommends Windows Server operating systems to prevent performance, stability, and scalability issues.

For evaluation purpose only CES can run under:

- Windows 10 Pro or Enterprise (with IIS 10)
  - CES 7.0.8047+ (December 2015)
- Windows 8.1 Pro or Enterprise (with IIS 8)
  - CES 7.0.6196+ (November 2013) Coveo .NET Front-End 12.0.446+ (November 2013)
- Windows 8 Pro or Enterprise (with IIS 8)
  - CES 7.0.4897+ (December 2012) Coveo .NET Front-End 12.0.61+ (December 2012)
- Windows 7 Professional, Enterprise, or Ultimate (with IIS 7)
2.6 Index Size

The index typically occupies 30% to 50% of the total size of the original documents.

Example: You index documents that occupy 1 TB in various repositories. With your mix of content type, the index size ends up at 42% of the original documents size (420 GB). The size of the dedicated index hard disk should be at least 500 GB.

- Dedicate a disk or disk set to the index files.
- Use local disks, direct-attached storage (DAS), or storage area network (SAN). Network-attached storage (NAS) as well as server message block (SMB) and other files shares are not supported.
- When a second index slice is required, you must install each slice on separate disk sets.
- RAID 0 and RAID 5 are not recommended.

Note: The index automatically switches to the read-only mode to prevent errors when the index disk free space reaches a minimum of 5 GB.

2.7 Non Index Files

For index sizes with more than 5 million documents, it is recommended to store non index CES files on a dedicated set of disks to separate inputs/outputs for these files from those for index slices.

The non index files are:

- Log files
- Default slice files
- Converter files
- Connector files
- Cache files
- Configuration files
- Certificate store files

Note: You will specify the path for these files following the CES installation when you create the index.

2.8 RAID Configuration

- It is recommended to create a RAID volume (a single accessible storage area) for each of the three categories of files:
  - OS and program files
  - Index files slice
2.9 Near Real-Time Indexing Disk

The Near Real-Time Indexing (NRTI) feature allows to make new documents searchable significantly faster for indexes with two million documents or more.

When you want to fully take advantage of this feature, because NRTI is I/O intensive, it is recommended to add a NRTI dedicated disk to your Coveo Master and Mirror servers that are serving queries and configure NRTI to use the dedicated disk.

The recommended disk specifications depend on the size of your index as shown in the first sub-sections of this topic.

2.10 Third-Party Software Requirement

The CES installer adds the following required software elements when not already installed:

- Microsoft .NET Framework 3.5 SP1 and 4.5.2 (side by side)
- Internet Information Services (IIS) 8 or 7
- Microsoft Chart Controls for Dotnet Framework 3.5 SP1
- Microsoft Visual C++ 2010 Redistributable Package (x64)

**Note:** Microsoft Visual C++ 2012 Redistributable Package (x64) is installed through the CES installer, which requires Microsoft Visual C++ 2010.

- MSXML 6
2.11 TLS/SSL Compatibility

Transport Layer Security (TLS) and its predecessor, Secure Sockets Layer (SSL), both of which are frequently referred to as "SSL", are cryptographic protocols that provide communications security over a computer network. Several versions of the protocols are in widespread use in applications such as web browsing, email, instant messaging, and voice-over-IP (VoIP).

Different versions of CES 7 offer a different support. Should your CES 7 version not support the right protocol version, it is strongly recommended that you upgrade to at least the lowest version that supports the protocol version that you need.

Example: You just installed Coveo .NET Frond-End on a new server. When you open the default search page, you receive the following message: The search interface is not available at this moment. Please try again later. If the problem persists, please contact your system administrator. When you ask for more details, you receive this message: The client and server cannot communicate, because they do not possess a common algorithm.

This is very likely to be linked to an incompatible cryptographic protocol.

The table below indicates which version of CES 7 is compatible with which cryptographic protocol.

<table>
<thead>
<tr>
<th>CES 7 Version</th>
<th>TLS 1.2</th>
<th>TLS 1.1</th>
<th>TLS 1.0</th>
<th>SSL 3.0</th>
</tr>
</thead>
<tbody>
<tr>
<td>Starting March 2016 (7.0.8225)</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>February 2015 (7.0.7402) to December 2015 (7.0.8047)</td>
<td>-</td>
<td>-</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>January 2015 (7.0.7338) and earlier</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>Yes</td>
</tr>
</tbody>
</table>

2.12 Relation Between CES Features and Hardware Resources

CES involves several processes that are running concurrently on one or more servers. Depending on the size of your Coveo installation, the activated features, and the phases of operation, these processes consume various levels of hardware resources.

The following list describes Coveo processes, components, or features that affect the hardware resources.

CPU

- Document conversion is entirely done in parallel. The greater number of CPU cores the better.
- Querying requires several CPU cores to perform as many steps in parallel.
- Queries with numerous terms, exact match operators, NEAR operator, or wildcard characters can take significant amount of CPU resources.

Note: You can configure the relative priority of the main, indexing, and crawling processes as well as specify the number of query threads.
Physical memory (RAM)

- Indexing uses a lot of physical memory to pre-compute mappings from terms to identifiers. More memory is better.
- Querying requires a good amount of physical memory for caches.
- Document conversion typically loads documents in physical memory.
- Numerous numerical fields often require to be kept in physical memory to achieve good query performance.
- Facet fields require an amount of physical memory directly proportional to the number of facet values to be cached. Not having enough memory to cache facets is not an option, as query performance would degrade significantly.
- String or numerical sorting fields have to be set up to be loaded in physical memory. For string sorting fields, the number of field items (cardinality) is what dictates how much memory is needed, the higher it is, the more memory it takes. For numerical sorting fields, cardinality doesn’t matter, only the number of documents in the index does.

Hard disk

- Indexing is disk I/O intensive. Upgrading the disk subsystem has the most impact for better performance.
- Querying is a process requiring a fast disk subsystem.
- Adding many string fields affects the disk subsystem, because it adds a lot of new terms to the index.
- Facet fields are easier to index when the number of different facet values is low (cardinality). The higher the cardinality, the higher the stress on the disk subsystem.
- String sorting fields put more stress on the disk subsystem than numerical fields.
- Document summarization produces a concept list and summary sentences that are added to the index.
- Document conversion accesses hard disk only for very large documents.

2.13 RAID Type Comparison and Recommendations

A redundant array of independent disks (RAID) is a technology that can be used to provide increased storage functions and reliability through redundancy. The following table provides a brief description of the common available RAID types and usage recommendation for CES.

<table>
<thead>
<tr>
<th>Type</th>
<th>Brief description</th>
<th>Recommendation</th>
</tr>
</thead>
<tbody>
<tr>
<td>RAID 0</td>
<td>Data striping without redundancy. Single disk failure destroys the array. High performance.</td>
<td>Not recommended since it is not fault tolerant</td>
</tr>
<tr>
<td>RAID 1</td>
<td>Mirroring. Provides better read performance than a single disk. Is fault tolerant.</td>
<td>Recommended for a single slice</td>
</tr>
<tr>
<td>Type</td>
<td>Brief description</td>
<td>Recommendation</td>
</tr>
<tr>
<td>----------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>--------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>RAID 10</td>
<td>Hybrid (or nested) RAID that is a stripe of mirrors (a RAID 0 of RAID 1). Performance is high for reads and writes. Is fault tolerant, as long as a mirror does not lose all its disks.</td>
<td>Recommended for two index slices</td>
</tr>
<tr>
<td>RAID 0+1</td>
<td>Offers a slightly better performance but is slightly less fault tolerant than RAID 10.</td>
<td>Recommended</td>
</tr>
<tr>
<td>RAID 5</td>
<td>Data striping with block level parity. Requires all drives but one to operate. Drive failure requires replacement. Read performance is adequate, but write performance is too low to be used in an indexing context.</td>
<td>Not recommended</td>
</tr>
<tr>
<td>RAID 1×n</td>
<td>A set of mirrors, one for each slice, when two slices are needed. Write and read performances are better because of the way CES evenly splits I/O operations between the RAID arrays. Basically, CES does the load-balancing instead of the controller. More complex configuration.</td>
<td>Recommended to achieve better performances with the same number of drives</td>
</tr>
</tbody>
</table>

2.14 Virtualized Server Guidelines

Coveo products can operate on virtual machines as they do on real hardware. As for real hardware, the key to a successful Coveo deployment on virtualized hardware is to respect the Coveo Platform requirements for the size of your index (see "Coveo Platform Hardware and Software Requirements" on page 3). Virtualized environments can vary greatly from one implementation to another so it is not appropriate to state specific virtual hardware requirements.

The nature of virtualized environments to optimize the usage of real hardware resources by sharing them among several virtual servers goes against the ideal setup where required resources are dedicated to a server. Like many processes, Coveo processes such as indexing documents or serving queries have varying server resource loads over time (see "Relation Between CES Features and Hardware Resources" on page 8).

You or some of your colleagues are experts on your hypervisor and virtual environment. You have the responsibility to ensure that your Coveo virtual server implementation maximizes the chances that required resources will be available when they are needed.

2.14.1 Guidelines

- Dedicate a virtual machine (VM) respecting the Coveo Platform requirements for your index size for each Coveo server (see "Coveo Platform Hardware and Software Requirements" on page 3).
- Minimize overcommitment of CPU and memory resources on a host where a virtual Coveo server is running.
- For large indexes, when your virtual environments does not allow you to create a virtual server that respects the requirements (see "Index From 40 to 80 Million Documents" on page 4), consider the following options:
○ Use geographically distributed indexing (GDI) to split the index in two or more CES instances, each on its dedicated virtual server (see "About Geographically Distributed Indexing" on page 20).

○ Commission a dedicated hardware Coveo server meeting the requirements.

• Disk management

Many Coveo processes are disk I/O intensive. The Coveo server requirements specify using separate dedicated disks for specific Coveo server process categories (operating system and programs, index, other Coveo files, and near-real time indexing) to optimize disk I/O performances and minimize interferences. In a virtual environment, the pool of available storage resources are not only shared among various processes of one server, but also with processes from several other servers.

Performance issues with virtual Coveo servers are often linked to poor disk performances.

Example: The Coveo server VM shares a disk resource with other host VMs, including a VM on which a large repository is hosted. The disk resource is able to respond to the average traffic.

However, when the Coveo server indexes the large repository, the disk resource throughput quickly reaches its limit because both the Coveo and the repository servers make significantly more disk I/Os, respectively to index the content, and to respond to the Coveo crawler. The performance of both systems (and any other host VMs sharing the same disk resource) drops significantly while indexing takes place.

You are the expert with your hypervisor and virtual environment:

○ Avoid sharing the same storage resources between a Coveo server and a repository that is indexed by Coveo.

○ Preferably use disk resources from a low latency storage area network SAN.

○ Attach available virtual disk resources (such as logical unit number [LUN] storage) that best match the requirements for your index size.

• Distribute Coveo intensive process schedules in time when shared resources are most available.

○ When you index more than one repository, avoid starting all source refreshes at the same time. Define source schedules that distribute source refreshes in time during off-peak hours.

Example: The default Every day source schedule starts every day at midnight. If all your daily refreshed sources use this schedule, they all start at midnight, potentially overloading your shared resources.

Rather create source specific (like Repository1 daily, Repository2 daily,...) or time specific (like Daily at 2:00 AM, Weekdays at 3:00 AM, Saturdays at 9:00 PM...) source schedules that you can assign to your sources to distribute the processes over the off-peak period.

○ Avoid scheduling Coveo intensive processes at the same time as other intensive processes (such as backups) from other systems.
3. Deployment

This section describes how to plan and roll out the deployment of your Coveo Platform implementation.

3.1 Coveo Platform Deployment Overview

The following list describes the main steps involved in the deployment of the Coveo Platform.

To deploy the Coveo Platform

1. Plan your deployment:
   a. Understand how the Coveo Platform can scale with increasing indexing and search needs (see "Coveo Scalability Model" on page 14).
   b. Identify and analyze the content of the repositories that you want to index (see "Planning Repositories to Index" on page 23).
   c. Determine the search interface needs for various groups of users (see "Planning .NET Search Hubs and Search Interfaces" on page 24).
   d. Determine if one or more Coveo servers are required and select the appropriate server topology and hardware (see "Coveo Platform Hardware and Software Requirements" on page 3).
   e. Determine ports to open

      Depending on the Coveo components you plan to use and your network configuration:

      i. Identify the required ports used by Coveo components you plan to use.
      ii. Identify special ports used by repositories you plan to index and needed by the Coveo connector to access the content.
      iii. Plan to have these ports opened by appropriate authorities in appropriate network infrastructure components such as firewalls.

      Example: Your CES Master server is deployed in a DMZ with search interfaces and repositories to index on either the internal or external side of the DMZ. You may need to open ports in both the internal and external side firewalls for the search interfaces and for the repositories.

2. Install the Coveo Enterprise Search Back-End components:
   a. Install the hardware for one or more Coveo servers for the selected topology.
   b. Install CES on the Master server, validate your Coveo license, and create an empty index or import the index configuration from your previous CES version (see "Installing CES on the Master Server" on page 28).
   c. When needed by your selected topology, add an index slice to the Master server.
   d. For a multiple server topology:
i. When your topology includes one or more Mirror servers, install the Coveo Mirror components (see "Installing CES Mirror Components" on page 57).

**Note:** By default, the remote converter components are installed on a Mirror server.

ii. When your topology includes one or more Remote Converter servers, install the Coveo Remote Converter components (see "Installing CES Remote Converter Components" on page 62).

iii. When two or more Master/Mirror servers are available, consider either of these options:

- Configure failover alternate servers (see "Configuring a .NET Front-End Server to Use Failover Alternate Back-End Servers" on page 100).

  OR

- Use a third-party solution to set them up in a network load-balancing configuration (see "Configuring Coveo Servers in a Network Load-Balancing Cluster" on page 98).

3. Populate the unified index:
   a. Create collections for your repositories.
   b. Create and crawl sources using the appropriate connectors for each repository.

4. Deploy at least one type of search interface:

   - Coveo JavaScript Search Framework and REST Search API
     Use the modern Coveo JavaScript Search with the REST Search API when you want developers to easily customize search pages.
     a. Because Coveo JavaScript Search pages communicate with CES through a REST search API, you must first install the search API.
     b. Create and deploy one or more JavaScript Search interface (see Getting Started with the JavaScript Search Framework).

   AND / OR

   - Coveo .NET Front-End
     Use the Coveo .NET Front-End when you want to get an out-of-the-box set of enterprise search interfaces that an administrator can customize using the .NET Interface Editor
     a. Install the Coveo .Net Front-End components on one or more Front-End servers of your selected topology. In the case of a one server topology, run the installer on the Master server only (see "Installing Coveo .NET Front-End" on page 43).
     b. When your topology includes two or more Front-End servers, consider setting them up in a network load-balancing configuration (see "Configuring Coveo Servers in a Network Load-Balancing Cluster" on page 98).
     c. Define one or more search hubs.
d. For each .NET search hub, select the .NET search interfaces to include.

e. For each .NET search interface, select options.

f. Consider deploying the Desktop Integration Package (DIP) on multiple workstations to allow users to take advantage of the Desktop Searchbar and the Outlook Sidebar (see "Desktop Integration Package Deployment Overview" on page 103).

3.2 Coveo Scalability Model

The Coveo Platform implementation can be easily scaled to serve the search needs for various enterprise sizes, from a single department to a large global international organization. The Coveo scalability model allows to operate either with a single Coveo server, with one Coveo instance composed of two or more Coveo servers, or with two or more inter-connected Coveo instances.

Note: Additional licensing is required for Coveo instances configured with more than one server.

3.2.1 One Server Configurations

In its simplest form, a Coveo instance is entirely hosted on one server that performs all the processes (crawling repositories, converting documents, hosting the index, hosting the search interface website, handling query requests, and returning query results).

![Diagram of Coveo Master server]

1. Coveo Master server
2. The default slice is always included in the Master server

3.2.2 Larger Number of Documents: Add a Slice

When the number of documents to index increases, hosting the index on a single hard disk leads to size and performance limitations. On one Coveo server, the index can be divided in up to two slices, each on a separate disk (see "About Index Slices" on page 18).
When the index size exceeds the capacity of one server, you can create other Coveo instances and federate search results (see "About Geographically Distributed Indexing" on page 20).

3.2.3 More Queries: Add Mirror and Front-End Servers

When one Coveo server handles all the CES processes and the rate of queries increases, the users may eventually feel that the system is slower, typically when the results are no longer returned within a second. Adding one or more Coveo Mirror servers allows supporting significantly more queries while maintaining sub-second response time 90% of the time. A Mirror server holds a copy of the master index and continuously receives updates from the Master server (see "About Mirror Servers" on page 18).

When IIS on the Master server is overloaded and cannot adequately serve search interfaces, one or more Coveo Front-End servers can also be added to distribute the website hosting of search interfaces and the handling of search queries.

The Master server and the Mirror servers are typically set up in a network load-balancing (NLB) configuration to provide optimized service availability and failover capability. For the same reasons, Front-End servers can also be set up in a separate NLB cluster.
Two Coveo Front-End servers in a network load-balanced cluster

The Coveo Master server with two Mirror servers in another network load-balanced cluster

Coveo Master server with up to two slices

First Coveo Mirror server with copies of the Master server slices

Second Coveo Mirror server with copies of the Master server slices

3.2.4 Heavy Document Conversion: Add Remote Converter Servers

When document conversion requires significant server resources, the document conversion process can be distributed to one or more Coveo Remote Converter servers to free the Coveo Master server from this task. This is useful for example when converting numerous documents involving the CPU and physical memory intensive optical character recognition (OCR) module.
3.2.5 Indexes in Various Locations: Set Up a Geographically Distributed Index (GDI)

Within an organization, separate Coveo instances may be distributed in different departments, buildings, cities, or even continents. Multiple Coveo instances can be set up to form a geographically distributed index (GDI). Queries entered in a search interface of one Coveo instance returns results gathered and ranked from two or more Coveo instances (see "About Geographically Distributed Indexing" on page 20).
3.2.6 About Index Slices

An index slice is a separate physical storage location for a part of the master index. The purpose of a slice is to distribute the master index content to increase the available space and to speed up the indexing process.

The Master server is always created with one slice named default. Adding a slice is necessary when the size of the disk limits the number of documents that can be indexed or when its performance affects the query response time. A slice must be added on separate disks on the Maser server.

Note: When all slices on your Master server are getting full, consider federating search on two or more Coveo instances (see "About Geographically Distributed Indexing" on page 20).

Index slices facts

- A slice can typically contain up to 40 million documents. One Coveo server can typically host up to two slices and contain up to 80 million documents. These numbers can however vary depending on a number of factors.
- Each slice should be created on a separate dedicated disk set.
- Slice files can also be hosted on a storage area network (SAN).
- Slices are filled in a distributed fashion so they grow with the same number of documents.

Note: When you add one slice, because the default slice is getting close to the limit, new documents will be added only to the new slice until it reaches the number of documents contained in the default slice. The documents are then distributed evenly in the two slices.

3.2.7 About Mirror Servers

A Coveo Mirror server hosts a copy of the master index located on the Coveo Master server. A Mirror server allows distributing queries between servers to speed up the querying process and to provide failover capability.

The process to add a Mirror server to a Coveo instance involves the following steps:

1. Installing the Coveo Mirror components on a dedicated server.
2. Configure the Coveo Master server to recognize and synchronize its index with remote Mirror server.
3. Configuring one or more Front-End servers to send queries to the new mirror server and to other available Back-End servers.

Mirror server facts

- The Coveo Master server hosts the master index. In the Administration Tool, the Master index is named the Default mirror.
- A Mirror server contains a copy of the master index, and therefore also duplicates the slice configuration of the Master server.
- A Master server sends index changes to the Mirror servers following its update schedules.
• The Coveo administrator can also schedule Mirror server updates, for example to off-peak hours.

• One Mirror server exclusively serving queries can typically respond to 25 queries per second (QPS), which can be adequate for several thousand concurrent users.

• Mirror servers provide a failover capability when the Master server and one or more Mirrors are configured in a network load-balancing (NLB) cluster. As long as one server is up and running, the system can return results to respond to incoming queries.

• You consider adding one or more Mirror servers:
  ○ When the query responses time increases notably (above one second) during peak usage because the Master server is busy with the multiple Coveo processes.
  ○ When you want to have query serving failover capability.
  ○ When you want to completely free the Master server from the query serving task.

Tip: You can add two or more Mirror servers in an NLB cluster, excluding the master server from the cluster, and sending all queries from the Front-End servers to the NLB cluster address.
3.2.8 About Geographically Distributed Indexing

Geographically Distributed Indexing (GDI) is a federated search feature which enables the communication between different Coveo instances. Its purpose is to deliver high search performance and availability, connecting unified indexes from offices distributed in different departments, sites, cities, or even countries around the world.

With GDI, a user makes a single query request in the search interface of the local Coveo instance. The query is distributed to the remote indexes participating in the federation. The local Coveo instance receives, merges, and ranks results from local and remote indexes before returning them to the user.

The Coveo scalability model supports two GDI configurations that are transparent to end-users.

**Query federated to the remote index**

In this configuration, the local Coveo instance sends federated queries to the remote indexes over the WAN (see "Setting up Geographically Distributed Indexing" on page 21).

This configuration is very simple to set up and has negligible impact on the WAN bandwidth. The query performance may however be affected by the time required for the round trip to the remote Coveo instance.

**Example:** Users working in the Palo Alto and Chicago offices must be able to search content from the Coveo instance in the other office. In the Palo Alto office, you configure the Coveo instance to accept queries from the Coveo instance in the Chicago office. In the Chicago office, you configure the Coveo instance to accept queries from the Coveo instance in the Palo Alto office.

**Query federated to a local mirror of a remote index**

In this configuration, you locally install a Coveo Mirror server of the remote index. You configure the remote Coveo instance to synchronize its index with this Mirror server over the WAN. The local Coveo instance sends federated queries to the local mirror of the remote index (see "Setting up Geographically Distributed Indexing Using a Mirror" on page 22).
Example: In the Palo Alto office, you deploy a Coveo Mirror server of the Chicago index office. You configure the Chicago Coveo instance to synchronize its index with the Palo Alto mirror server. You configure the Palo Alto Coveo instance to use the mirror server as the Chicago remote index. In the Chicago office, you can do the same thing for the Palo Alto office.

Note: When connecting two indexes in a GDI configuration, it is a good practice to keep the index field configuration as similar as possible in the two indexes to prevent problems.

Example: The `@systemstatus` field is present or is configured as a facet field only in one of the indexes. When you create a facet with this field in a Coveo .NET Front-End search interface, you can get an error similar to the following one:

```
"Call returned SOAP fault class CES::SearchServerException: class CES::SearchServerException: class Merlin::KIEException: class Merlin::KIEInvalidFacetField: The field is not a facet field or is a field that cannot be optimized (@systemstatus)."
```

3.2.8.1 Setting up Geographically Distributed Indexing

You can easily create a one way interconnection between a local and a remote Coveo instance to create a geographically distributed index (GDI) using the CES remote index features (see "About Geographically Distributed Indexing" on page 20).

The configuration consists in enabling the remote Coveo instance to accept remote queries, add the remote index to the local Coveo instance, and configure a local search interface to include results from the remote index. Users from the local Coveo instance can then search content in the remote index.

Note: You can create a two-way interconnection between Coveo instances by repeating the following procedure for the other direction.
To set up a geographically distributed index

1. Ensure that the Coveo instances that you want to interconnect meet the following requirements:
   - All Coveo instances of the geographically distributed indexing setup must reside on the same domain.
   - The CES search application pool for the local Coveo instance must run under a domain account. It is a best practice to create a dedicated account for this purpose with a strong password that never changes.

2. On the Coveo Master server of the local Coveo instance:
   a. Add the remote index.
   b. Configure a scope that includes the remote index.

3. On the Coveo Front-End server of the local Coveo instance, assign the scope that includes the remote index to the desired .NET search interface.

4. Using the .NET search interface for which you modified the scope, perform queries to validate that content from the remote index is returned.

   **Tip:** If needed, on the Coveo Master server of the remote Coveo instance, open the CES Console to validate that the remote index receives the queries sent from the local .NET search interface.

3.2.8.2 Setting up Geographically Distributed Indexing Using a Mirror

You can set up geographically distributed indexing using a local mirror of a remote index (see "About Geographically Distributed Indexing" on page 20).

   **Note:** You can create a two-way interconnection between Coveo instances by repeating the following procedure for the other direction.

To set up a geographically distributed index using a mirror

1. Ensure that the Coveo instances that you want to interconnect meet the following requirements:
   - All Coveo instances of the geographically distributed indexing setup must reside on the same domain.
   - The CES search application pool for the local Coveo instance must run under a domain account. It is a best practice to create a dedicated account for this purpose with a strong password that never changes.

2. Physically install a local server and install the Coveo Mirror software components without the web interfaces.

3. For the remote Coveo instance, configure the Master server to recognize and synchronize its index with your new local Mirror server.

4. On the Coveo Master server of the local Coveo instance:
   a. Add the remote index.
   b. Configure a scope that includes the remote index.

5. On the Coveo Front-End server of the local Coveo instance, assign the scope that includes the remote index to the desired .NET search interface.
6. Using the .NET search interface for which you modified the scope, perform queries to validate that content from the remote index is returned.

**Tip:** If needed, on the Coveo Master server of the remote Coveo instance, open the CES Console to validate that the remote index receives the queries sent from the local .NET search interface.

### 3.3 Planning Repositories to Index

Bringing structured and unstructured data from multiple repositories in one unified index is the great benefit of the Coveo Platform. When a unified index is available, the Coveo solutions allow you to search, consolidate, correlate, and analyze information from emails, knowledge based documents, customer relation management (CRM) system, database entries, people information, etc.

One of the basic tasks when planning a Coveo installation is to identify all the repositories that you want to index within your organization. Coveo Enterprise Search (CES) can index many types of repositories and supports many specific systems.

Analyze the content of each repository:

- Estimate the number of documents in the repository.
- Estimate the total size of the original documents
- List the main types of repository documents.

**Example:** Microsoft Office, PDF, text, html, email, database records…

- Identify if some content requires special conversion tools.

**Example:** Text extraction using optical character recognition (OCR) in images.

- For email repositories and desktops, estimate the number of users.
- Estimate the yearly growth for:
  - Number of documents
  - Number of users

Note the values for each repository in a table similar to the following one and contact the Coveo Support to help you plan your Coveo installation.

<table>
<thead>
<tr>
<th>Repository</th>
<th>Documents</th>
<th>Users</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type</td>
<td>Example</td>
<td>Number</td>
</tr>
<tr>
<td>Email</td>
<td>Microsoft Exchange Lotus Notes Enterprise Vault</td>
<td></td>
</tr>
</tbody>
</table>

www.coveo.com
<table>
<thead>
<tr>
<th>Repository</th>
<th>Documents</th>
<th>Users</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Type</td>
<td>Number</td>
</tr>
<tr>
<td>Web pages</td>
<td>Example</td>
<td></td>
</tr>
<tr>
<td>Website</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Extranet</td>
<td></td>
<td></td>
</tr>
<tr>
<td>File share</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Network drives</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Local files</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Deskspos</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Laptops</td>
<td></td>
<td></td>
</tr>
<tr>
<td>People information</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Microsoft Active Directory</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Database</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Microsoft SQL Server</td>
<td></td>
<td></td>
</tr>
<tr>
<td>CMS</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Microsoft SharePoint</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Sitecore</td>
<td></td>
<td></td>
</tr>
<tr>
<td>CRM</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Salesforce</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Wiki</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Confluence</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### 3.4 Planning .NET Search Hubs and Search Interfaces

The Coveo Platform comes with a set of feature-rich out-of-the-box .NET search interfaces that you can use immediately.

Coveo .NET Front-End makes search interfaces available through search hubs that contain one or more .NET search interfaces. Each .NET search interface has its own search scope and presents appropriate content.

**Examples:** While the All Content .NET search interface searches all indexed repositories, the Intranet .NET search interface returns result from your SharePoint farm, and the People .NET search interface consolidates people information from Microsoft Active Directory and Microsoft Outlook contacts.

When different groups of people have different search needs, you can create different search hubs that include appropriate search interfaces for each group, and control the access to each .NET search hub.

**Example:** When you want that only people from the marketing, sales, and management departments have access to the CRM search interface, you can include this interface only in a search hub to which only these people have access. If this is the only exclusive search interface, you only need one other search hub for everybody else.

CES integrates and indexes document-level permissions of each repository. This means that for each repository, only documents to which a user has access are returned in the search results. Consequently, you do not need to create different search hubs for one shared repository.
Example: On a shared network file server, if a HR folder access is restricted to people from the human resources department, the connector that crawls the whole file server indexes the access restriction together with the documents. When searching the network file server content, only human resources employees will see search results from the HR folder.

To plan search hubs and interface

1. List all the repositories that you want to index (see "Planning Repositories to Index" on page 23).
2. Review the out-of-the-box .NET search interfaces that you can use to search all or specific repositories.
3. When the access to one or more .NET search interface must be restricted:
   a. Identify the .NET search interfaces to which you want to restrict the access.
   b. Create a list of search hubs, their .NET search interfaces, and the access restriction to each hub.
4. Note the information in a table similar to the following example and contact the Coveo Support to help you plan your Coveo Platform installation.

<table>
<thead>
<tr>
<th>Search hub</th>
<th>Search interfaces</th>
<th>Access restriction</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sales &amp; marketing</td>
<td>My Emails</td>
<td>Marketing, Sales, Management</td>
</tr>
<tr>
<td></td>
<td>My Files</td>
<td></td>
</tr>
<tr>
<td></td>
<td>People</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Intranet</td>
<td></td>
</tr>
<tr>
<td></td>
<td>CRM</td>
<td></td>
</tr>
<tr>
<td></td>
<td>File Share</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Extranet</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Knowledge Base</td>
<td></td>
</tr>
<tr>
<td></td>
<td>All Content</td>
<td></td>
</tr>
<tr>
<td>General</td>
<td>My Emails</td>
<td>All employees</td>
</tr>
<tr>
<td></td>
<td>My Files</td>
<td></td>
</tr>
<tr>
<td></td>
<td>People</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Intranet</td>
<td></td>
</tr>
<tr>
<td></td>
<td>File Share</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Knowledge Base</td>
<td></td>
</tr>
<tr>
<td></td>
<td>All Content</td>
<td></td>
</tr>
<tr>
<td>Website</td>
<td>Website</td>
<td>All web users</td>
</tr>
</tbody>
</table>

3.5 Installing Coveo Platform Software Components

This section contains procedures describing how to install the various on-premises Coveo Platform software components (see "About Back-End and Front-End Component Versions" on page 27).

The procedures that you need to perform depend on the server topology that you selected (see "Coveo Platform Deployment Overview" on page 12).
3.5.0.0.1 Coveo for Sitecore case

**Important:** When you want to use Coveo within a Sitecore site, deploy Coveo for Sitecore (see Coveo for Sitecore Installation and Upgrade Guide).

3.5.0.0.2 Single-server case

1. Download the latest CES version (x64) from the Coveo website.

   **Note:** Contact Coveo Support when you need the 32-bit version.

2. Install Coveo Enterprise Search (CES), the main back-end component hosting your index (see "Installing CES on the Master Server" on page 28).

3. Install at least one type of search interface:
   a. Use the Coveo JavaScript Search when you want developers to easily customize search pages (see Getting Started with the JavaScript Search Framework). Because Coveo JavaScript Search pages communicate with CES through a REST search API, you need to first install the search API.
   b. Use the Coveo .NET Front-End when you want to get an out-of-the-box set of enterprise search interfaces that an administrator can customize using the .NET Interface Editor (see "Installing Coveo .NET Front-End" on page 43).

3.5.0.0.3 Multiple-server cases

1. Download the latest CES version (x64) from the Coveo website.

   **Note:** Contact Coveo Support when you need the 32-bit version.

2. Install Coveo Enterprise Search (CES), the main back-end component hosting your index on a dedicated machine (see "Installing CES on the Master Server" on page 28).

3. When you want one or more servers responding to queries, install one or more Mirror servers on separate dedicated machines (see "Installing CES Mirror Components" on page 57).

4. Install at least one type of search interface:
   a. Use the Coveo JavaScript Search when you want developers to easily integrate and customize a search page into one or more websites or repositories (see Getting Started with the JavaScript Search Framework). Coveo JavaScript Search pages communicate with CES through a REST search API, so you need to also deploy the search API somewhere, typically on a back-end server.
   b. Use the Coveo .NET Front-End when you want to deploy out-of-the-box enterprise search interfaces on one or more front-end servers (see "Installing Coveo .NET Front-End" on page 43).

   You can also integrate Coveo .NET Front-End in SharePoint.

3.5.0.0.4 Optional Module cases

If you acquired optional modules install them:

→ www.coveo.com
- Desktop Integration Package (DIP)
  You can centrally deploy the DIP to install the Coveo Desktop Searchbar and the Outlook Sidebar in local workstations (see "Desktop Integration Package Deployment Overview" on page 103).

- Text Analytics module
  You can create metadata from unstructured content using the Text Analytics module.

- OCR module
  You can index the text appearing in images with the optical character recognition (OCR) module (see "Installing the Optical Character Recognition Module" on page 69).

### 3.5.1 About Back-End and Front-End Component Versions

The Coveo Platform Back-End and Front-End components are released separately. They are deployed using separate installers and are identified with different version numbers.

**Note:** Once Back-End and Front-End components are installed, you can identify the current installed versions respectively from the Administration Tool and .NET Interface Editor.

<table>
<thead>
<tr>
<th></th>
<th>Back-End</th>
<th>.NET Front-End</th>
</tr>
</thead>
<tbody>
<tr>
<td>Product name</td>
<td>Coveo Enterprise Search (CES)</td>
<td>Coveo.NET Front-End</td>
</tr>
<tr>
<td>Version number format</td>
<td><img src="https://via.placeholder.com/150" alt="Example" /></td>
<td><img src="https://via.placeholder.com/150" alt="Example" /></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>7.0.4678</td>
<td>12.0.23</td>
</tr>
<tr>
<td><strong>Note:</strong></td>
<td>The first major release number was arbitrarily set to 12.</td>
<td></td>
</tr>
</tbody>
</table>

#### Included servers
- Coveo Master, Mirror, and Remote Converter
- Coveo.NET Front-End, SharePoint integration

#### Included tools
- Administration Tool
- CES Console
- Optional:
  - Usage Analytics Module
  - OCR Module
- Interface Editor
- Optional: Desktop Integration Package (DIP)
3.5.2 Installing CES on the Master Server

The Coveo Enterprise Search (CES) installer allows you to deploy all Back-End components. You must install CES on the Master server first. In the case of a one server installation, this is the only Back-End installation that is required. In a multiple Back-End server topology, you must run the CES installer on each Back-End Server (see "Coveo Platform Deployment Overview" on page 12).

**Note:** If you are updating CES to a new minor or monthly release (7.x.nnnn), refer to "Upgrading CES" on page 79.

To install CES on the Master server

1. Before you start the installation, ensure to perform the following preparation steps:
   
   a. Install the hardware for a server that fulfills the Coveo system requirements. In particular, ensure to install the recommended dedicated disk(s) for the index (see "Coveo Platform Hardware and Software Requirements" on page 3).
   
   b. Decide which existing or new Windows account to use as the CES service logon account.
   
   c. Decide which CES service port (default 52800) to use.
   
   d. Ensure to open the ports used by the Coveo Platform.
   
   e. Determine if you want to convert an existing CES 6 index configuration or create a new index.
   
   f. Locate the email message received from Coveo that contains your Coveo license that you will need to provide during the installation.

   **Note:** You do not receive your license key by email if you are installing CES as a part of the Coveo for Sitecore 4 setup. The license is configured subsequently by the Coveo for Sitecore 4 installation wizard itself (see Installing Coveo for Sitecore).
Important: For an installation on Windows Server 2008 where the User Account Control (UAC) is activated, ensure to keep a backup copy of the CES installer. While the UAC is activated, uninstalling CES only works using the original installer executable.

2. When not already done, download the latest CES version (x64) from the Coveo website.

Notes:
- Contact Coveo Support when you need the 32-bit version.
- The CES installer creates a website in IIS for the Administration Tool.
- The CES installer enables ASP.NET pages on the IIS Web server.
- The Coveo installers require the .NET Framework 2 that is usually available on Windows Server OS.

3. Using a local administrator account, connect to the server on which you want to install CES.

4. Locate and run the CES installer that you downloaded.

Example: When the installer is in your Downloads folder, run: `C:\Users\Username\Downloads\Coveo Enterprise Search 7.0 x64 (nnnn).exe`

5. **CES 7.0.6547+ (March 2014)** When Microsoft .NET Framework 4.5 SP1 is not available on your server, a Coveo Enterprise Search 7 Setup dialog box appears. Click Install to download and install the missing Microsoft .NET Framework component.

Important: The Microsoft .NET Framework installer will require that you restart the server following this installation when no prior Microsoft .NET Framework 4.5 version was installed on your server.

![Coveo Enterprise Search 7 Setup](image)

Note: The Microsoft components are installed through the Internet. When the installer does not have access to the Internet, prerequisite installations will fail. You must then install the components manually and restart the CES installer.

6. When a Coveo Enterprise Search 7 Setup dialog box as shown below appears, click Install to install the other...
components that CES also needs.

7. Wait for the component installation to complete.

8. In the Coveo Enterprise Search 7.0 Installation Welcome screen, click Next.

9. In the License Agreement screen, read the license terms, select I accept the terms in the license agreement, and then click Next.

10. In the Select Setup Type screen:

- Click Typical to install CES in the default installation folder (C:\Program Files\Coveo Enterprise Search 7\).

OR
a. Click Custom when,

- You want to specify a CES installation folder other than the default.

  **Example:** Your IT rules may specify that on servers, only the operating system can be installed on the C: hard disk drive and all other software must be installed on the D: hard disk drive.

- You must install the Admin Service, such as when you install CES on a Sitecore 7 server to be used with Coveo for Sitecore.

b. In the **Installing Folders** screen:

i. For a Coveo Master server, ensure to select to install the following components and their child components:

   - **Coveo Enterprise Search Server**
   - **Console**

ii. Select to install **Admin Service** only when you need this service such as when you install CES for Coveo for Sitecore.
Notes:

- **CES 7.0.6339+ (January 2014)** The Admin Service option to install the Admin Service is available and not selected by default.
  
  **CES 7.0.6225– (December 2013)** The Admin Service is always installed.
  
- Once installed, the Coveo Admin Service is available as a Windows service.

iii. **CES 7.0.8388+ (June 2016)** (For Coveo for Sitecore only) Select to install a standalone version of RabbitMQ.
  
  **Note:** The RabbitMQ option is not selected by default.

iv. Select Coveo Enterprise Search Server, and then under Location, click Change.

v. In the Modify Current Destination Folder screen, select the desired installation folder for CES, and then click OK.

  **Example:** D:\Program Files\Coveo Enterprise Search 7\

vi. Click Next.

  **Note:** Because the Coveo Enterprise Search installation folder may be different from one implementation to another, it is referred to as the [CES_Path] variable in the documentation.

**Note:** The Advanced option is used when you want to create Coveo Mirror or Remote Converter servers (see "Installing CES Mirror Components" on page 57 and "Installing CES Remote Converter Components" on page 62).

11. In the Configuration screen, click Configure next to Account used to access the files to index.
12. In the **Service Logon Account** screen, select the account that CES uses to run its service:
a. In the **Username**, **Password**, and **Domain** boxes, enter the credentials of the account that you want to use for the CES service.

**Note:** It is recommended to create and use a Windows administrator account dedicated to CES with a strong password that never changes.

b. Click **OK**.

**Note:** CES 7.0.6424+ (February 2014) The Use local system account in order to only index local files option no longer exists because selecting this option can lead to various authentication issues.

13. Back in the **Configuration** screen, when you need to change the default port used by the CES service (52800), click **Configure** next to **CES service port**.

**Example:** You need to change the port when you install CES 7 on the same server as your CES 6 instance. Two CES instances can reside on the same server but they must use different CES service ports.

In the **CES Service Configuration** screen:

a. In the **Port** box, type the desired port number (ex.: 52801).

b. Click **OK**.

14. Back in the **Configuration** screen, click **Configure** next to **Web site hosting the Administration Tool**.

15. CES 7.0.8388+ (June 2016) Back in the **Configuration** screen, when you need to change the default Web site
name and port (Coveo Enterprise 7 Admin, port 8081), click Configure next to Website hosting the Administration Tool.

**Note:** CES 7.0.8225– (March 2016) You need to validate the default Web site name and port.

16. In the **Web Interface Configuration** screen, configure the website that hosts the Administration Tool:

![Web Interface Configuration Screen](image)

a. In the **Web site name** box, enter a name that you want to see in IIS for the website. The default is Coveo Enterprise Search 7 Admin.

b. In the **Web site port** box, when the default port value (8081) is in conflict with another process on the server, enter the port that you want to use.

c. Click **OK**.

17. **CES 7.0.6547+ (March 2014)** Back in the **Configuration** screen, when you chose to install the Admin Service, the **Admin service security** option appears. It is then recommended to click Configure next to **Admin service security** to secure the Admin Service and prevent anonymous usage of the service.

**Notes:**

- **CES 7.0.6424– (February 2014)** The Admin Service was only accessible anonymously.

- When you use the Admin service security to be used with Coveo for Sitecore, you need to perform additional configuration .

18. In the **Coveo Enterprise Search Admin Service Security Options** screen:
a. Select the **Enable Coveo Enterprise Search Admin service security** check box.

**Important:** When the Admin Service is installed, it is highly recommended to activate the security to restrict access users or processes that can authenticate with the credentials that you provide below. Otherwise, anyone can use the service to perform administrative tasks on your CES instance.

When secured, the service is available through HTTPS, by default on port 443. A certificate must be bound to the port to allow the connection (see [Securing the Admin Service - Troubleshooting](#)).

b. **CES 7.0.8388+ (June 2016)** When the default **Admin Service port number** (443) is used by another service or application, modify the port number.

c. **CES 7.0.7814+ (August 2015)** Next to **Configure credentials for the Admin Service**, click **Configure**.
d. In the **Username**, **Password** and **Confirm Password** boxes, enter credentials that you create and take good note of them.

The specified username/password do not need to be that of an Active Directory or Sitecore user. They are encrypted and stored only on the Coveo server. These credentials will be used by application (such as the Coveo for Sitecore Search Provider) that need to authenticate to the Admin Service.

e. Click **OK**.

f. **CES 7.0.7814+ (August 2015)** Next to **Configure a certificate for the Admin Service**, click **Configure**.

**Important**: The certificate validity period depends on your CES version:

- **CES 7.0.8147– (December 2015)** The certificate is valid for two years (see "Extending CES Admin Service Certificate Validity Period" on page 86).
- **CES 7.0.8225+ (March 2016)** The certificate is valid for 50 years.
g. In the **Create a certificate to secure the Admin Service** screen, configure the certificate settings:

i. In the **CES Server name** box, enter the fully qualified domain name (FQDN) of the CES server or an alias for future reference using your hosts file.

   **Note:** The default value is the computer name.

ii. In the **Certificate private key password** and **Confirm Password** boxes, enter the password to protect the certificate private key.

iii. **CES 7.0.8225 (March 2016)** When the default **Admin Service port number** (443) is used by another service or application, modify the port number.

iv. Optionally click **Browse** to modify the default **Certificate export path**, which is the Coveo Enterprise Search 7 folder, and then click **OK**.

v. Click **OK**.

19. **CES 7.0.7256+ (December 2014)** Back in the **Configuration** screen, click **Configure** next to **RabbitMQ username and password**.

20. In the **RabbitMQ Security Options** screen, create RabbitMQ administrator credentials:
a. Select the **Set RabbitMQ administrator credentials and overwrite default values** check box.

**Important:** The default user id/password is guest/guest. For evident security reasons, create new RabbitMQ default administrator credentials.

b. In the **Username** and **Password** boxes, enter credentials that you create and take good note of them.

**Notes:**
- You will need these credentials when installing Coveo for Sitecore and/or when accessing RabbitMQ management.
- You can also change the password once RabbitMQ is installed.

c. Click **OK**.

21. Back in the **Configuration** screen, click **Next**.
22. In the **Installing the program** screen, click **Install**.
23. Wait for the installation to complete while a screen shows the installation progress bar.
24. In the installer **Installation Successful** screen, click **Finish**.
The Coveo Diagnostic Tool Setup Wizard is automatically launched after a Coveo Enterprise Search installation or update (see Installing the Coveo Diagnostic Tool).

What's Next?

- In the case of an upgrade for a dot or build release, the procedure ends here.
- In the case of a new installation, the installer automatically launches the Create Index page of the Administration Tool to allow you to create an empty index or import the configuration of an existing CES 6 index (see "Creating a New Index or Importing an Existing CES 6 Index Configuration" on page 40).
- If the case of a Coveo for Sitecore setup, go back to the step Installing the Coveo Search API in the Coveo for Sitecore installation guide.

3.5.3 Creating a New Index or Importing an Existing CES 6 Index Configuration

After installing CES on the Coveo Master server the first time, you need to create a new empty CES 7 index or import the configuration of an existing CES 6 index. The CES installer automatically opens the Administration Tool Create Index page at the end of the first CES 7 installation.

**Note:** The Administration Tool Create Index page is only accessible at the initial setup or in the extreme case where you start the Administration Tool after deleting or renaming the [Index_Path] folder.

**Important:** You can import your CES 6 index configuration, but because the CES 7 index has been improved and its format is not compatible with that of CES 6, you will need to rebuild all your sources in CES 7.

To create a new index or import an existing CES 6 index

1. In the Create index page of the Administration Tool that appears at the end of the CES first time installation, under Index Creation, select one of the following two options:

   - **Create a new index**

     Choose this option when you are installing CES on a new server.
a. Under **Index Files Location**, in the **Index Folder** box, click `...` to browse or type the path where you want to store the index files on the server. The default is `C:\CES7`.

**Important:** It is recommended to create the index files on a physical disk other than the one where the operating system resides to maximize CES performances (see "Coveo Platform Hardware and Software Requirements" on page 3).

**Example:** You installed a `D:` drive on the server for the index files. Enter `D:\CES7` to create the index on this drive rather than on the OS and programs `C:` drive.

**Note:** The folder entered in this box is referred to as the [Index_Path] in the documentation.

b. Expand **Advanced Options** to review and adapt default paths for various CES configuration folders.

c. Under **Advanced Options**, enter the full path for each of the specific file types.

**Important:** For large index sizes, it is recommended to dedicate a disk or set of disks to the non index files (see "Non Index Files" on page 6).
It is recommended to use the default file paths but to change the drive letter to match the one of the dedicated disks.

CES 7.0.7022+ (September 2014) It is recommended to configure the Near Real-Time Indexing Folder and Near Real-Time Indexing Cache Folder on the same dedicated disk (see "Near Real-Time Indexing Disk" on page 7).

Example: You installed a E: drive on the server for the non index files. In the Log Files Folder box, click to browse or type E:\CES7\Log. Repeat the edit for all other Advanced Options folders.

d. In the Services Port box, change the default Coveo Search Web Service port (52810) only when this port is used by another process on the server (see Search SOAP API Home).

Note: The Coveo Search Web Service was introduced with CES 7.0. You can therefore use the default port even when a CES 6 instance is present on the server.

e. Click Create Index.

OR

• Convert an existing CES 6 index configuration

Choose this option when you are migrating from CES 6 and want to rebuild the index in CES 7 using the sources defined in the configuration of the existing CES 6.

Under Conversion Parameters, perform the following steps:

a. In the CES 6 Index Folder box, click to browse or type the path of the existing CES 6 index on this server.

Note: When your CES 6 index configuration is on another server, make a copy of the CES 6 configuration on this server.

b. In the CES 7 Index Folder box, use the default path (C:\CES7) or click
... to browse or type a new path name where the new CES 7 index will be created.

**Important:** The index performance is better when the index is created on a physical hard disk other than the one where the operating system and the swap files reside (see "Coveo Platform Hardware and Software Requirements" on page 3).

c. Click **Create Index**.

**Note:** Because the index folder may be different from one implementation to another, it is referred to as the [Index_Path] variable in the documentation.

What's Next?

The **Enter License Code** page of Administration Tool opens automatically to let you enter your Coveo license information.

3.5.4 Installing Coveo .NET Front-End

**Note:** When you run the Coveo .NET Front-End installer on a SharePoint server to integrate Coveo into your SharePoint site, the procedure is different.

A Coveo Front-End server holds only the .NET search interfaces, not the index. A Front-End server connects to one or more Coveo Back-End servers (Master or Mirror) to query the unified index that they contain. You can however install the Coveo Front-End and Back-End components on the same server, like in the case of a single server topology.

The Coveo .NET Front-End installer creates a website in IIS for the .NET search hub and .NET search interfaces.

**Note:** Installing Coveo .NET Front-End enables ASP.NET pages on the IIS Web server.

To install Coveo .NET Front-End on your the front-end server

1. Ensure that the server hardware meets the Coveo system requirements (see "Coveo Platform Hardware and Software Requirements" on page 3).

2. When not already done, download the latest version of Coveo .NET Front-End (32-bit or x64 version) from the Coveo website.

**Notes:**

- You can download the latest version of Coveo .NET Front-End from the Coveo Product Updates page.
- The Coveo .NET Front-End 12.0 is compatible with CES 7 and CES 6.5.

3. Using a local administrator account, connect to the server on which you want to install Coveo .NET Front-End.

4. Locate and run the Coveo .NET Front-End installer that you downloaded.

**Example:** When the installer is in your Downloads folder, run: C:\Users\Username\Downloads\Coveo .NET Front-End 12.0 x64 (22).exe

5. When a required version of Microsoft .NET Framework is missing on the server, the **Coveo Enterprise Search**
7 Setup dialog box that appears, click Install.

**Note:** The Microsoft components are installed through the Internet. When the installer does not have access to the Internet, prerequisite installations will fail. You must then install the components manually and restart the CES installer.

6. When a Coveo Enterprise Search 7 Setup dialog box appears to propose to install other required third-party components missing on the server, click Install.

The Microsoft .NET Framework components installation progress bar appears.

7. In the Welcome screen of the Coveo .NET Front-End 12.0 installer, click Next.

8. In the License Agreement screen, read the license terms, select I accept the terms in the license agreement, and then click Next.

9. In the Installing Folders screen:

   i. When you want to install the Coveo .NET Front-End software in a folder different from the default folder (C:\Program Files\Coveo .NET Front-End 12), under Location, click Change.

   ii. In the Modify Current Destination Folder screen, select the desired installation folder, and then click OK.

      **Example:** D:\Program Files\Coveo .NET Front-End 12\

   iii. Click Next.

   **Note:** Because the Coveo .NET Front End installation folder may be different from one implementation to another, it is referred to as the [.Net_Front-End_Path] variable in the documentation.

10. In the Configuration screen, click Configure next to Web site hosting the interfaces.
11. In the **Web Interface Configuration** screen, configure the website that hosts the web .NET search interfaces:

![Image of Web Interface Configuration screen]

- In the **Web site name** box, enter a name that you want to see in IIS for the website. The default is Coveo .NET Front-End 12.

  **Note:** This name appears only in IIS and is not visible to end-users.

- In the **Web site port** box, when the default port value (8080) is in conflict with another process on the server, enter the port that you want to use.

- Click **OK**.

  **Note:** When you set up more than one Front-End server, to make the administration simpler, it is recommended to use the same website configuration for all Front-End servers.

12. Back in the **Configuration** screen, click **Configure** next to **Coveo Enterprise Search server and port**.

![Image of Configuration screen]
13. In the **CES Configuration** screen:

![ CES Configuration Screen ](image)

a. In the **Server name** box, enter the hostname of the Coveo Back-End server (where CES is installed) to which you want to connect this Front-End server. You can leave `localhost` when CES is also installed on the current server.

b. In the **Service port** box, change the CES service port default (52810) only when needed.

c. Click **Test Server**, refer to the information in the dialog box that appears to verify if the specified CES server responds and is compatible with the Coveo .NET Front-End version that you are installing, and then click **OK**.

d. Click **OK**.

14. Back in the **Configuration** screen, click **Next**.

15. In the **Installing the program** screen, click **Install**.
Important: When you are upgrading the Front-End server to a new minor or build release, click Yes in the following dialog box only when you are certain that it is not a problem to temporarily interrupt the Coveo search interface service for your end-users.

A screen showing the installation progress bar appears.

16. In the Installation Successful screen, click Finish.

What's Next?

When you install Coveo .NET Front-End for the first time on a server, before you can use .NET search interfaces, you must link the Front-End to a Back-End server. In this case, the Coveo .NET Front-End installer automatically opens the Front-End Server Configuration page (see "Coveo .NET Front-End First Time Setup" on page 47).

Note: Ensure that a firewall on the Coveo Front-End server allows communications for the port used by the .NET search interface. The default .NET search interface port is 8080.

3.5.5 Coveo .NET Front-End First Time Setup

When you install the Coveo .NET Front-End components for the first time on a server, the installer automatically accesses the search page at the end of the installation process. The Front-End Server Configuration web page appears to allow you to complete the Front-End first time setup.

As a Coveo administrator, you can also access the Front-End Server Configuration page again later from the .NET search interface Do more menu.
Notes:

- In some cases, such as with Claims authentication, the **Do more** menu **Configure Front-End** item does not appear even when you are an administrator. In such a case, you can access the **Front-End Server Configuration** page directly using the page URL in the form:

  
  
  http://[MyCoveoFrontEndServer]:8080/Coveo/FirstTimeSetup/default.aspx

  
  or when the search page is integrated in SharePoint:

  http://[MySharePointServer]/_layouts/Coveo/FirstTimeSetup/

- The URL used to access the **Front-End Server Configuration** page is also used to automatically set the pre-loading URL on the Back-End server. The pre-loading URL is used to warm up the Front-End search page, eliminating longer loading time for end-users.

  
  When the Front-End and Back-End components are installed on separate servers, if you can, use a search URL that the Back-end server can resolve to access the **Front-End Server Configuration** page and correctly set the pre-loading URL.

  

  
  Otherwise, a warning message appears (Back-End and Front-End components appear to be installed on separate servers. You may need to change the default pre-loading search page URL from the Administration Tool in the Configuration > Pre-loading page.).

In the **Front-End Server Configuration** page, you must provide administrator credentials to configure the Back-End server that this Front-End server uses to send queries and receive search results. You can also select or create the search security certificate used to secure the connection between the Front-End and Back-End processes.

**Coveo .NET Front-End 12.0.49+ (September 2012) CES 7.0.4855+ (August 2012)** When the Coveo search interface is installed on a server that uses Claims to authenticate users (such as a SharePoint server), you must also provide Claims parameters.

**To perform the Coveo .NET Front-End first time configuration**

1. In the **Front-End Server Configuration** page, the **Front-End Server Settings** section appears only when the current user does not have administrator permissions on the Front-End server.

   **Example:** The **Front-End Server Settings** section appears when you access the **Front-End Server Configuration** page from a Coveo .NET search interface installed on a SharePoint server that uses Claims to authenticate users.
a. In the **Username** and **Password** boxes, enter the credentials of an administrator account on the Front-End server to be able to save the configuration performed in this page.

b. Click **Login**.

2. In the **Coveo Enterprise Search Server Settings** section that appears:

![Coveo Enterprise Search Server Settings](image)

a. In the **Connection Information** section:

i. In the **Hostname** box, enter the hostname of the Coveo Master server, where Coveo Enterprise Search (CES) is installed.

   When the Coveo Front-End component is installed on the same server as the Coveo Master server, you can use localhost. When they are on different servers, enter the hostname of the Master server, even when you want to connect this Front-End server to a Mirror server (you will select the Mirror server later in this page).

ii. In the case where your Coveo Master server uses a Coveo Search Web Service other than the default (52810), expand the **Advanced setting** section, and in the **Services Port**, enter the appropriate value.

   **Note:** Do not confuse this port with the CES service port. The Front-End uses the Coveo Search Web Service to get additional configuration information from the Back-End server, including the CES service port (52800 by default) that the .NET search interface will use to communicate with the server.

iii. Click **Validate server information**.

   When the connection is established successfully, a green indicator (✓) appears next to the button.
When the connection cannot be completed, a red indicator and message (Invalid server information) appear next to the button and an error message appears at the top of the page. In this case, adjust the connection information and try again.

b. In the Administrator Credentials section that appears:
   
i. In the Username and Password boxes, enter the credentials of a Coveo administrator account for the Coveo Master (Back-End) server.
   
ii. In the Provider drop-down list, select the security provider that can validate these user credentials, most likely Active Directory.
   
iii. Click Login.

3. **Coveo.NET Front-End 12.0.1548+ (June 2016)** When you want users of the search page you are configuring to be able to see content from a SharePoint server configured with Claims authentication, the Coveo .NET Front-End search page hosted outside SharePoint must authenticate each SharePoint end-user performing queries.

   In such a case, in the Claims SSO for SharePoint Settings section:

```
<table>
<thead>
<tr>
<th>Claims SSO for SharePoint Settings</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Claims SSO Configuration</strong></td>
</tr>
<tr>
<td><img src="https://example.com" alt="Checkbox: Import claims SSO config from SharePoint claims identity provider setup page" /></td>
</tr>
<tr>
<td><img src="https://example.com" alt="Warning: It is strongly recommended to browse this page in privacy mode and over a secured (https) connection to protect the sensitive security information contained in the claims SSO configuration." /></td>
</tr>
</tbody>
</table>

   Claims SSO Configuration to Import:

   ![Clipboard of claims SSO configuration text](https://example.com)

   ![Import and Validate the Configuration button](https://example.com)
```

   a. Select the Import the claims SSO configuration from the SharePoint claims identity provider setup page check box.

   b. In the Claims SSO Configuration to Import box, paste the claims SSO configuration that was generated in the SharePoint claims identity provider setup page.

4. In the Mirror Settings section:

```
<table>
<thead>
<tr>
<th>Mirror Settings</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="https://example.com" alt="Checkbox: Select a mirror" /> <img src="https://example.com" alt="Checkbox: Configure mirror manually" /></td>
</tr>
<tr>
<td><img src="https://example.com" alt="Default Mirror option" /></td>
</tr>
</tbody>
</table>
```

![www.coveo.com](https://example.com)
When your Coveo implementation does not include Mirror servers:

Select the Select a mirror option, and in the drop-down box, leave Default.

When your Coveo implementation includes one or more Mirror servers:

You can decide to which Mirror server this Front-End server sends queries.

Example: When you want to free the Master server from handling the queries, you can rather connect the Front-End to a Mirror server.

Tip: When you have two or more Coveo Front-End servers, you can later set them up in a network load-balancing cluster.

- Select the Select a mirror option, and in the drop-down box, select the mirror to which you want this Front-End server to send the queries.

OR

a. When you configured your Mirror server to use a CES service port other than the default (52800), select the Configure mirror manually option.

b. In the Mirror Hostname box, enter the Mirror hostname, otherwise, enter the same machine name as in Hostname.

c. In the Mirror Port box, enter the port that your Mirror server uses.

5. When the Coveo .NET search page is installed on a server such as SharePoint that uses Claims to authenticate users or when the Claims SSO for SharePoint is enabled, in the Claims-Based Authentication Settings section that appears:
a. **Coveo .NET Front-End 12.0.1633+ (September 2016)** In the **Claims Security Provider** drop-down lists, select the claims security providers that you created for these Claims-based Front-End servers.

**Note:** **Coveo .NET Front-End 12.0.1548– (June 2016)** Only one **Claims Security Provider** is supported for your Claims-based Front-End servers.

**Example:** You could index content from a Claims-based on-premises SharePoint server and also from SharePoint Online. You need to create one Claims security provider for each of these SharePoint instances.

**Note:** The following message appears when no Claims security provider is available:

A Claims Security Provider is required, add one with the Administration Tool.

b. In the **Active Directory Security Provider** drop-down list, select the Active Directory security provider to use.

c. In the **Claim type holding Active Directory users** list, the first claim is automatically selected, typically in the **DOMAIN\username** form, and is generally the best choice. Consider selecting another claim when the first one does not work.
Note: Coveo .NET Front-End 12.0.1459– (March 2016) With previous versions, the Claim type holding Active Directory users list provided many more claims to select from.

- When you want end-users to be able to search for documents from other sources that were crawled in an Active Directory environment, select the Claim Type to use to resolve an Active Directory identity from a Claims identity. You must select a Claim Type that has a Claim Value Example in the MyDomain\UserName or UserName@MyDomain.com form. Only the Claim Type is saved and used to get the Claim Value for each user when they perform queries.

- When end-users can only search for Claims protected documents, you can select (None).

6. In the Search Certificate Settings section that appears:

   a. For Select or create the search certificate to use to be trusted when communicating with the Back-End server select one of the following options:

   **Use the default certificate**

   The default certificate trusts everyone that has access to the .NET search interface and the Front-End server can be any machine (any IP address).

   **Use an existing certificate**

   When you already created one or more search security certificates on the Back-End server, select the desired certificate in the list that appears.
Create a new certificate

Use this option to create a certificate to trust only specific users and/or groups and trust only servers with specific IP addresses.

b. When you select **Create a new certificate**, use the parameters that appear to build the certificate:

- In the **Name** box, enter a name for your new search security certificate.
- In the **Trusted Users/Groups** section, optionally define the trusted users:
  - Select **Specific user and/or groups** when you want this certificate to trust only specific users.
  - In the **Name** box, enter the name of a user or group to be trusted.
  - In the **Type** drop-down list, select if the name is for a user or group.
  - In the **Provided** drop-down list, select the security provider in which this user or group is defined.
  - Click **Add**.
The specified user or group appears in the list.

F. When you want to add other trusted users or groups, repeat the previous steps.

iii. In the **Trusted Front-End Servers** section, define the IP address for one or more Front-End servers to be trusted by the Back-End server:
   a. Select **Specific IP addresses** when you want this certificate to trust only specific machines.
   b. In the **IP address** box, enter an IP address to be trusted.
   c. Click **Add**.

The specified IP address appears in the list.

D. When you want to add other trusted Front-End servers, repeat the previous steps.

7. In the **Search Analytics Settings** section, you can optionally configure this search front-end server to send search usage information to an on-premises database and/or to the Coveo Usage Analytics cloud service to later be able to review search usage data:

**Notes:**

- **Coveo .NET Front-End 12.0.1548+ (June 2016)** .NET Framework 4.5 is required on the Coveo Front-End server to push information to the Coveo Usage Analytics cloud service.
- **CES 7.0.7711+ (June 2015)** Support for sending analytics to the Coveo Usage Analytics cloud service.

a. When you have access to a deployed on-premises Coveo Analytics module, in the **On-Premises Analytics Module** section:
   i. Select the **Enable** check box.
   ii. In the **Database Connection String** box, enter the connection string for the database of your Analytics module.
   iii. Click **Test** to validate the string.

b. **Coveo .NET Front-End 12.0.1548+ (June 2016)** When you have access to the Coveo Usage Analytics cloud service, in the **Cloud Platform** section:
   i. Select the **Enable** check box.
   ii. Depending on your setup, select one on the following radio button:
      - In a non-NLB (Network Load Balancing) setup, select the **Push usage analytics information directly to the Coveo Usage Analytics cloud service** radio button.
      - In an NLB setup, select the **Push usage analytics information directly to the Coveo Usage Analytics cloud service** radio button on one .NET Front-End server, and the **Delegate pushing usage analytics information to another Coveo .NET Front-End NLB server** radio button on the
other(s).

Notes:

- For high-volume environments, the best practice is to set up a separate .NET Front-End server, outside the NLB, and whose only responsibility is to push events to the cloud service.
- The URI of the Front-End(s) on which the Delegate pushing usage analytics information to another Coveo .NET Front-End NLB server radio button is selected should point to the Front-End that pushes the events to the cloud service.

iii. Depending on the radio button you select:

- When you select the Push usage analytics information directly to the Coveo Usage Analytics cloud service radio button, in the API Key box, enter the API key to be used to call the Usage Analytics REST endpoint, and then click Test to validate the endpoint.

  **Note:** Contact Coveo Support to get an API key.

- When you select the Delegate pushing usage analytics information to another Coveo .NET Front-End NLB server radio button, in the box, enter the URL of the Coveo .NET Front-End to delegate pushing usage analytics information to in the following form:

  http://[CoveoFrontEndServer]:8080/PushCloudAnalyticsInfo.aspx

8. Click Apply Settings.

9. Enable the Front-End that pushes UA information to the Coveo Usage Analytics cloud service to log errors in a folder of your choice:

  **Note:** Error logs are a good starting point when investigating problems.

a. Using a text editor, open the Web.config file (by default: C:\Program Files\Coveo .NET Front-End 12\Web.config).

b. In the file, add the logFolder parameter (in red) in the analytics section as follows:

```xml
<analytics enabled="False" connectionString="Data Source=yourServerName;Initial Catalog=CoveoAnalytics;Integrated Security=SSPI;" cloudEnabled="True" logFolder="D:\[folderPath]" platformEndpoint="" analyticsEndpoint="https://usageanalyticsdev.coveo.com/rest/v13" accessToken="YOURACCESSSTOKEN" analyticsCloudDelegateUrl="http://YOURHOSTNAME:8080/PushCloudAnalyticsInfo.aspx" analyticsCloudDelegateEnabled="False" />
```

The first time setup is completed and the default .NET search interface appears.
What's Next?

You can now customize or create search hubs and .NET search interfaces using the .NET Interface Editor.

3.5.6 Installing CES Mirror Components

When your selected Coveo server topology includes one or more Mirror server (see "About Mirror Servers" on page 18), you must install the Coveo Enterprise Search (CES) mirror components on each Mirror server.

**Note:** By default, the remote converter components are also installed with the mirror components. You can therefore also use a Mirror server to take over the documents conversion process and reduce the load on Master server.

To install CES on a Mirror server

1. Ensure that a master index is already installed on a Coveo Master server.

2. Ensure that your Coveo software license that includes a Mirror.
   
   The license is only validated on the Master server but must include the option allowing the Master server to send index data updates to the Mirror server.

3. Ensure that the hardware of the server you want to use as a Mirror server meets the Coveo system requirements. In particular, ensure to install the recommended dedicated disk(s) for the index (see "Coveo Platform Hardware and Software Requirements" on page 3).

4. Using an administrator account, connect to the server on which you want to install the CES Mirror components.

5. Locate and run the same CES installer that you downloaded and used for the Master server. The Mirror and Master servers must run the same CES major.minor.build version.

   **Example:** When CES 7.0.4772 is installed on the Master server, on a 64-bit server, use the Coveo Enterprise Search 7.0 x64 (4772).exe installer.

   **Note:** You can download the latest version of Coveo Enterprise Search (CES) from the Coveo Product Updates page.

6. When a Coveo Enterprise Search 7 Setup dialog box as shown below appears, click Install to install the other
components that CES also needs.

Note: The Microsoft components are installed through the Internet. When the installer does not have access to the Internet, prerequisite installations will fail. You must then install the components manually and restart the CES installer.

7. In the Welcome to Coveo Enterprise Search 7.0 screen of the installer, click Next.

8. In the License Agreement screen, read the license terms, select I accept the terms in the license agreement, and then click Next.

9. In the first Select Setup Type screen, click Advanced.

10. In the second Select Setup Type screen, select Mirror and Remote Converter, and then click Next.
11. In the Configuration screen, click Configure next to Account used to access the files to index.

12. In the Service Logon Account screen, select the account that CES uses to run its service:
In the Username, Password, and Domain boxes, enter the credentials of the account that the Coveo Master server uses for the CES service, and then click OK.

**Note:** All Coveo Master and Mirror servers must use the same logon account.

13. Back in the Configuration screen, when you need to change the Mirror server name and/or the default port used by the CES service (52800), click Configure next to Name of the mirror.

In the Mirror Configuration screen:
a. The server host name appears by default in the Mirror name box. You can enter another name. The name must include only alphanumeric characters, a dash (-) or a dot (.), no spaces or other special characters.

b. In the Port box, type the desired port.

Example: If this server is also a CES 6 Mirror server that already uses port 52800, you need to change the port so that the two CES instances can reside on the same server. You can use port 52801.

c. Click OK.


15. In the Installing the program screen, click Install.

A screen showing the installation progress bar appears.

16. In the installer Installation Successful screen, click Finish.

What's Next?

You must now configure your Coveo Master server to use this new Mirror server.

You can also configure your Coveo Master server to use this new Mirror server as a Remote Converter server.
3.5.7 Installing CES Remote Converter Components

Converters are responsible for converting documents to the common format used by the index. A CES converter handles the supported document types.

By default, the CES remote converter components are installed on Mirror servers (see "Installing CES Mirror Components" on page 57). When you have a lot of documents to convert, you can also install only the CES remote converter components on one or more servers to distribute the converting process between CPUs and, therefore, speed up indexing.

**Important:** For an installation on Windows Server 2008 where the User Account Control (UAC) is activated, ensure to keep a backup copy of the CES installer. While the UAC is activated, uninstalling CES only works using the original installer executable.

To install CES remote converter components on a server

1. Ensure that the hardware for the server fulfills the Coveo system requirements (see "Coveo Platform Hardware and Software Requirements" on page 3).

2. Using a local administrator account, connect to the server on which you want to install the CES remote converter components.

3. Locate and run the same CES installer that you downloaded and used for the Master server. The Remote Converter and Master servers must run the same CES major.minor.build version.

**Example:** When CES 7.0.4772 is installed on the Master server, on a 64-bit server, use the Coveo Enterprise Search 7.0 x64 (4772).exe installer.

**Note:** You can download the latest version of Coveo Enterprise Search (CES) from the Coveo Product Updates page.

4. When a dialog box as shown below appears, click **Install** to install the Microsoft components that the CES Remote Converter needs. These installations can take several minutes.
Note: The Microsoft components are installed through the Internet. When the installer does not have access to the Internet, prerequisite installations will fail. You must then install the components manually and restart the CES installer.

5. In the Welcome to Coveo Enterprise Search 7.0 screen of the installer, click Next.

6. In the License Agreement screen, read the license terms, select I accept the terms in the license agreement, and then click Next.

7. In the first Select Setup Type screen, click Advanced.

8. In the second Select Setup Type screen, select Remote Converter, and then click Next.
9. In the **Installing the program** screen, click **Install**.

   A screen showing the installation progress bar appears.

10. In the installer **Installation Successful** screen, click **Finish**.

### What’s Next?

You must now configure your Coveo Master server to use this new Remote Converter server.

### 3.5.8 Installing or Updating CES Silently

Advanced users can use the Coveo Enterprise Search (CES) install kit, which is a standard Windows Installer package (.msi file) wrapped in a self-extracting archive, to install or update CES without having to go through dialogs. The install kit is launched using `msiexec`, the Windows installer executable that comes with all Windows installations.

**Note:** This feature is useful in a large scale deployment in which you need to install or update CES on different machines with the same or mostly the same parameters.

**Important:** The Coveo Support team will not provide any assistance regarding this procedure.

To install CES silently

1. With an administrator account, log in to the target machine.

2. Ensure the machine meets the following requirements:
- Coveo Enterprise Search (CES) 7.0 (available on the Coveo website)

  **Note:** You must use an archiving software such as WinRAR or 7-zip to extract the .msi file from the application (.exe).

- Microsoft Windows Installer version 3.1 or more recent (already included in Windows).

- Microsoft .NET Framework 3.5 SP1

  **Note:** Depending on the version of the exploitation system on which runs the target machine:
  - When running on Windows Server 2008 or Windows Vista, see Microsoft .NET Framework 3.5 Service Pack 1.
  - When running on Windows Server 2008 R2 or Windows 7 or subsequent Windows version, see How to install/enable .Net 3.5 SP1 on Windows Server 2008 R2 for SQL Server 2008 and SQL Server 2008 R2.

- Microsoft .Net Framework 4.5.2 (see Microsoft .NET Framework 4.5.2)

  **Note:** These two major versions of Microsoft .NET Framework (3.5.1 and 4.5.2) are working side-by-side.

- Microsoft Chart Controls (see Microsoft Chart Controls for Microsoft .NET Framework 3.5)

- Internet Information Services (IIS) (see Installing IIS 7 on Windows Server 2008 or Windows Server 2008 R2)

  **Note:** All role services must be installed.

- MSXML 6 (x64 or 32-bit)

- Microsoft Visual C++ Redistributable 2010 (x64 or 32-bit)

3. Disable User Access Control for both an install or an update (see Turn User Account Control on or off).

4. When your machine runs on Windows Server 2012/Windows 8 and subsequent, set the EnableLUA registry key to 0:
   a. Click the Windows Start button, and then type and select Run.
   b. In the Run window, in the Open box, enter regedit.exe and then click OK.
   c. In the Registry Editor window, access the System folder (HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System).
   d. In the System folder, open EnableLUA, and then change the value in the Value data box to 0.
   e. Restart the machine.

5. Once the machine is restarted, open a text editor.

6. In the text editor, build a command line:
a. Since the installation is launched using msiexec.exe, start your command line with msiexec (see Msiexec (command-line options)).

b. The parameter to install or update the software is /i, followed by the installer package file path and the parameter for a silent installation is /qn.

   Note: After these two sub-steps, your command line should look like the following:

   msiexec/i "C:\[FilePath]\Coveo Enterprise Search 7.0 x64 (nnnn).msi" /qn

c. For installation only, depending on your setup:

   Notes:
   
   - The syntax to respect is the following: [VARIABLE]=[Value].
   - Values are separated by commas.
   - Variables are separated by spaces.
   - Variable names are case sensitive.
   
i. Using the ADDLOCAL variable, ensure the command line contains the required CES features:

   Tip: A typical installation includes the following features: CESService, CESConsole, Admin, AdminService (only for Sitecore integrations), DiagnosticTool, BaseFeature and VCRedist.

<table>
<thead>
<tr>
<th>Features</th>
<th>Description</th>
<th>Is required</th>
</tr>
</thead>
<tbody>
<tr>
<td>Admin</td>
<td>Web application used to configure Coveo Enterprise Search</td>
<td>No (but recommended)</td>
</tr>
<tr>
<td>AdminService</td>
<td>The Coveo Admin Service</td>
<td>Only in Sitecore Integration setups</td>
</tr>
<tr>
<td>DiagnosticTool</td>
<td>The Coveo Diagnostic Tool</td>
<td>No</td>
</tr>
<tr>
<td>CESService</td>
<td>The master Coveo Enterprise Search service</td>
<td>No (if CESMirror is installed)</td>
</tr>
<tr>
<td>CESMirror</td>
<td>The mirror Coveo Enterprise Search service</td>
<td>No (if CESService is installed)</td>
</tr>
<tr>
<td>CESConverter</td>
<td>Converts documents for the Coveo Enterprise Search Server</td>
<td>No</td>
</tr>
<tr>
<td>CESConsole</td>
<td>Tool to monitor the Coveo Enterprise Search Server</td>
<td>No (but recommended)</td>
</tr>
<tr>
<td>BaseFeature</td>
<td>Set of files required for the installation</td>
<td>Yes</td>
</tr>
<tr>
<td>VCRedist</td>
<td>Microsoft Visual C++ Redistributable 2012</td>
<td>Yes</td>
</tr>
</tbody>
</table>
ii. Add the required options that have no default value (LOGONACCOUNT_DOMAIN, LOGONACCOUNT_USERNAME and LOGONACCOUNT_PASSWORD) and optionally add others, or modify default option value(s):

**Note:** When options are not included in the command line, their default value is taken into account.

**Important:** It is recommended to only use or modify options that you are familiar with. A misuse of options can make CES unusable, and some options can even impact your target machine environment.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Default</th>
<th>Description</th>
<th>Is required</th>
</tr>
</thead>
<tbody>
<tr>
<td>ISSITECORE</td>
<td>0</td>
<td>Set this parameter to 1 to install RabbitMQ along with CES.</td>
<td>No</td>
</tr>
<tr>
<td>INSTALLLOCATION</td>
<td>&quot;C:\Program Files\Coveo Enterprise Search 7&quot;</td>
<td>Installation folder for the application</td>
<td>Yes</td>
</tr>
<tr>
<td>NEW_WEBSITE_NAME</td>
<td>&quot;Coveo Enterprise Search 7 Admin&quot;</td>
<td>The name of the web site that will be automatically created</td>
<td>Yes</td>
</tr>
<tr>
<td>NEW_WEBSITE_PORT</td>
<td>8080</td>
<td>The port used for the new web site</td>
<td>Yes</td>
</tr>
<tr>
<td>NEW_WEBSITE_IP</td>
<td>*</td>
<td>IP address of the new website (&quot; stands for &quot;All Unassigned&quot;)</td>
<td>Yes</td>
</tr>
<tr>
<td>LOGONTYPE</td>
<td>account</td>
<td>The type of logon used for the service</td>
<td>Yes</td>
</tr>
<tr>
<td>LOGONACCOUNT_DOMAIN</td>
<td></td>
<td>The domain of the account</td>
<td>Yes</td>
</tr>
<tr>
<td>LOGONACCOUNT_USERNAME</td>
<td></td>
<td>The user name used to log on</td>
<td>Yes</td>
</tr>
<tr>
<td>LOGONACCOUNT_PASSWORD</td>
<td></td>
<td>The password of the account</td>
<td>Yes</td>
</tr>
<tr>
<td>SERVICES_PORT</td>
<td>52800</td>
<td>The port used by the CES service (or the slice or mirror depending on the installation)</td>
<td>Yes</td>
</tr>
<tr>
<td>SKIP_CHK_CES_READY_FOR_UPGRADE</td>
<td>false</td>
<td>Use this flag to skip the check for mirrors availability when performing an upgrade.</td>
<td>Yes</td>
</tr>
<tr>
<td>Variable</td>
<td>Default</td>
<td>Description</td>
<td>Is required</td>
</tr>
<tr>
<td>------------------------------------------------------</td>
<td>----------------------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>-------------</td>
</tr>
<tr>
<td>USE_ADMIN_SERVICE_SECURITY</td>
<td>CES 7.0.6547+ (March 201)</td>
<td>(For a Sitecore integration only) Define this property and the two following ones to activate Admin Service security.</td>
<td>No</td>
</tr>
<tr>
<td>ADMINSERVICELOGON_USERNAME</td>
<td>CES 7.0.6547+ (March 201)</td>
<td>(For a Sitecore integration only) If using Admin Service security, set the username to use. Will be inserted in the security configuration file.</td>
<td>No</td>
</tr>
<tr>
<td>ADMINSERVICELOGON_PASSWORD</td>
<td>CES 7.0.6547+ (March 201)</td>
<td>(For a Sitecore integration only) If using Admin Service security, set the password to use. Will be hashed and inserted in the security configuration file.</td>
<td>No</td>
</tr>
<tr>
<td>ADMIN_SERVICE_PORT</td>
<td>CES 7.0.6547+ (March 201)</td>
<td>(For a Sitecore integration only) If using Admin Service security, set the port to use. Will be inserted in the security configuration file. The service usually uses port 443.</td>
<td>Yes</td>
</tr>
<tr>
<td>ADMIN_SERVICE_CERTIFICATE_EXPORT_PATH</td>
<td>Typically C:\Program Files\Coveo Enterprise Search 7</td>
<td>Use this parameter to set the Admin Service certificate path to a specific output folder.</td>
<td>No</td>
</tr>
<tr>
<td>ADMIN_SERVICE_CES_SERVER_NAME</td>
<td>[YOUR HOST NAME]</td>
<td>Use this parameter to set a specific name for the certificate pfx file.</td>
<td>No</td>
</tr>
<tr>
<td>ADMIN_SERVICE_PRIVATE_KEY_PASSWORD</td>
<td>CES 7.0.6547+ (March 201)</td>
<td>Use this parameter to set a password to secure the certificate private key. It can be an empty string.</td>
<td>No</td>
</tr>
<tr>
<td>SKIP_SERVICES_CHECK</td>
<td>CES 7.0.6767+ (June 2014)</td>
<td>When defined, will not fail the installation if the CES service fails to start.</td>
<td>No</td>
</tr>
</tbody>
</table>

d. Once done, copy the command line.
Note:

- A typical installation command line:
  
  ```
  msiexec /i "C:\[FilePath]\Coveo Enterprise Search 7.0 x64 (nnnn).msi" /qn
  ADDLOCAL=BaseFeature,VCRedist,CESService,Admin,AdminService,CESConsole
  LOGONTYPE=account LOGONACCOUNT_DOMAIN=[domain] LOGONACCOUNT_USERNAME=[username] LOGONACCOUNT_PASSWORD=[password]
  ```

- A typical update command line:
  
  ```
  msiexec /i "C:\[FilePath]\Coveo Enterprise Search 7.0 x64 (nnnn).msi" /qn
  ```

Example: When you are installing CES in a Coveo for Sitecore setup, the certificate creation for the admin service is mandatory. The typical installation command line looks like the following:

```
msiexec /i "C:\[FilePath]\Coveo Enterprise Search 7.0 x64 (nnnn).msi" /qn
ADDLOCAL=BaseFeature,VCRedist,CESService,Admin,AdminService,CESConsole
ISSITECORE=1 LOGONTYPE=account LOGONACCOUNT_DOMAIN=[domain] LOGONACCOUNT_USERNAME=[username] LOGONACCOUNT_PASSWORD=[password] USE_ADMIN_SERVICE_SECURITY=Yes ADMIN_SERVICE_PORT=443 ADMINSERVICELOGON_USERNAME=coveoservice
ADMINSERVICELOGON_PASSWORD=[password]
```

7. Once your command line is done, open **Command Prompt** as an administrator.

8. In the **Command Prompt**, paste and execute the command line.

9. Ensure Coveo Enterprise Search (CES) is correctly installed.

3.5.9 Installing the Optical Character Recognition Module

The Coveo Enterprise Search (CES) Optical Character Recognition (OCR) module is optional. You must install the module separately from CES.

When you purchased the OCR module, your CES license includes authorization for the module. You will need the CES license file that you received by email to complete the installation of the OCR module.

To install the OCR module

1. Using an administrator account, connect to the Coveo Master server (where Coveo Enterprise Search is installed).

2. In your emails, find and open the **Coveo Enterprise Search License Information** email message that you received from Coveo (cesSales@coveo.com):
   
   a. Using the link provided in the email message, download the appropriate (x 32 or x 64) OCR module installer.

   ```
   Note: The latest version of the OCR module installer is always available from the Coveo download site for both 64-bit or the 32-bit version.
   ```
b. Using a text editor, open the Coveo Enterprise Search License Code.txt file attached to the email message.

**Note:** If you are updating the OCR module from the 32-bit to the 64-bit version, first uninstall the 32-bit OCR module.

3. On the Coveo Master server, run the OCR module installer.

4. In the installer Welcome to Coveo Enterprise Search OCR Module 7.0 screen, click Next.

5. In the installer License Agreement screen, read the license agreement, select I accept the terms in the license agreement, and then click Next.

6. In the installer Installation Folder screen:
   - Click Next to use the default installation folder.
   - OR
   - Click Browse to select another folder, and then click Next.

7. In the installer License Configuration screen:
   a. In your text editor, from the Coveo Enterprise Search License Code.txt file, copy the license text, ensuring that you include the {BEGIN LICENSE} and {END LICENSE} tags.
   b. In the installer screen, paste the license text in the text box.
   c. Click Next.

8. If a User Account Control dialog box appears, click Yes to accept the installation of this software on your computer.

9. Wait for the installation to complete.

10. In the installer Setup Complete screen, click Finish.

**Note:** When you update CES, it is recommended to also run the OCR module installer to also update the OCR module.

What's Next?

You must create an OCR open converter.

3.5.10 Modifying, Repairing, or Uninstalling CES Components

Once Coveo Enterprise Search (CES) components are installed on a server, you can run again the same installer to modify or repair installed CES components or completely uninstall CES from the server.
To modify, repair, or uninstall CES components

1. Using an administrator account, connect to the server on which you want to modify, repair, or uninstall CES components.

2. Locate and run the same CES installer that you used to install the currently installed CES components.

   **Example:** When CES 7.0.4772 is currently installed on a 64-bit server, use the Coveo Enterprise Search 7.0 x64 (4772).exe installer.

   **Notes:**
   - Running a newer installer version would rather be an upgrade (see "Upgrading CES" on page 79).
   - You cannot run an older installer version, you would first need to uninstall the current version.

3. In the installer welcome screen, click **Next**.

4. In the installer **License Agreement** screen, read the license terms, select **I accept the terms in the license agreement**, and then click **Next**.

5. In the installer **Select Maintenance Type** screen:

   - **Modify**
     - Allows users to add or remove features.
   - **Repair**
     - Reinstalls the features currently installed.
   - **Remove**
     - Removes Coveo Enterprise Search 7.0 (x64) completely.

Click one of the following option and refer to the appropriate section below:
- **Modify**
  To add or remove CES components such as the **Admin Service**, the **Diagnostic Tool**, the **Mirror**, the **Remote Converter**, or the **Console**.

- **Repair**
  To reinstall and optionally change the configuration of currently installed CES components such as:
  - If and where to back up customized files
  - The account used to by the CES service
  - If the Admin Service security is enable and what are the access credentials

  **Note**: CES 7.0.7711+ (June 2015) Changing the configuration of the Admin Service security is no longer possible during a repair.
  - The Diagnostic Tool website port

- **Remove**
  To completely remove Coveo Enterprise Search and all associated components from your server.

3.5.10.0.0.1 Modify Option

To add or remove CES components on this server:

a. Click **Modify**.

b. In the **Installing Folders** screen, expand the drop-down list of the features that you want to add or remove.
i. To add a component, click **This feature will be installed on local hard drive** OR **This feature, and all subfeatures, will be installed on local hard drive**.

ii. To remove a component, click **This feature will not be available**

iii. Click **Next**.

c. In the **Configuration** screen, click **Next**.

d. In the **Installing the program** screen, click **Install**.

   A screen showing the installation progress bar appears.

   e. In the installer **Installation Successful** screen, click **Finish**.

   OR

   3.5.10.0.0.2 Repair Option

   To reinstall and optionally change currently installed CES components:

   a. Click **Repair**.

   b. In the **Configuration** screen:
When you want to configure if and where CES files that you modify are backed up:

A. Next to **Backup customized files**, click **Configure**.

B. In the **Backup Customized Files** screen, when you want to have backups, select the **Backup customized files to the following folder** check box, click **Change** to choose the backup folder.
ii. When **Not configured** appears under **Account used to access the files to index** or when you want to change the logon account of the CES service, next to it, click **Configure**, and then in the **Service Logon Account** screen:

**Tip:** You can also change the CES service logon account from the Microsoft Windows **Services**.
A. In the Username, Password, and Domain boxes, enter the credentials of the Active Directory account with which the CES service will run.

**Important:** All Coveo Master and Mirror servers must use the same logon account.

B. Click OK.

iii. When the CES Admin Service is installed (see "Modify Option" on page 72) and you want to change its security configuration, next to Admin service security (optional), click Configuration, and then in the Coveo Enterprise Search Admin Service Security Options screen:
A. It is highly recommended to select the **Enable Coveo Enterprise Search Admin service security** to secure the service.

**Important:** When the Admin Service is installed, it is highly recommended to activate the security to restrict access users or processes that can authenticate with the credentials that you provide below. Otherwise, anyone can use the service to perform administrative tasks on your CES instance.

When secured, the service is available through HTTPS, by default on port 443. A certificate must be bound to the port to allow the connection (see [Securing the Admin Service - Troubleshooting](#)).

B. In the **Username** box, enter a CES Admin Service username of your choice.

**Note:** The user name and the password that you specify do not need to be linked with any system (such as Active Directory). These credentials are encrypted and stored in the CES Admin Service configuration.

C. In the **Password** and **Confirm password** boxes, enter a password of your choice.

D. Take note of these credentials in a safe location, so that you can find them when you need to
access the CES Admin Service.

E. Click OK.

iv. When you need to change the Diagnostic Tool port, next to Diagnostic Tool web site port, click Configuration, and then in the Coveo Diagnostic Tool Web Site Configuration screen:

A. In the Port Number box, enter the desired port number. The default value is 52580.

B. Click OK.

c. Back in the Configuration screen, click Next.

d. In the Installing the program screen, click Install.

A screen showing the installation progress bar appears.

e. In the installer Installation Successful screen, click Finish.

OR

3.5.10.0.0.3 Remove Option

To uninstall all the CES components currently installed on this server:

a. Click Remove.

b. In the Configuration screen, when you want to also delete the CES data files from the server:

   i. Next to Delete configuration and index files, click Configure.

   ii. In the Delete Data Files screen, select the Delete the Coveo Enterprise Search 7.0 (x64)
configuration and index files check box, and then click **OK**.

![Coveo Enterprise Search 7.0 (x64) Installation](image)

A feature selected for uninstallation has created configuration and index files. Do you want these data files to be deleted? It is recommended to keep the files if you plan on reinstalling the Coveo Enterprise Search 7.0 (x64) feature at a later time.

- **Delete the Coveo Enterprise Search 7.0 (x64) configuration and index files**

| OK | Cancel |

- **c.** Back in the **Configuration** screen, click **Next**.
- **d.** In the **Ready to uninstall the program** screen, click **Uninstall**.

A screen showing the uninstallation progress bar appears.

- **e.** In the **Installation Successful** screen, click **Finish**.

### 3.5.11 Upgrading CES

You can easily upgrade Coveo Enterprise Search (CES) to a newer minor or monthly release version using the installer on Coveo servers.

**Example:** You can upgrade from CES 7.0.4781 to 7.0.4784, a new monthly release of the same minor version of CES 7.

The CES installer can perform the upgrade typically in less than 15 minutes, but the upgrade process involves restarting the CES service process. During the few minutes the CES service is stopping and restarting, no queries will be served. If you do not have another Coveo Back-End server (Master or Mirror) set up in a load balancing configuration or a Front-End failover setup, consider performing the upgrade during an off-peak search period (see "Configuring Coveo Servers in a Network Load-Balancing Cluster" on page 98 and "Configuring a .NET Front-End Server to Use Failover Alternate Back-End Servers" on page 100).
In short, the installer detects the folder of the current installation, backs up the configuration, sets the index in read-write mode if it is currently in read-only mode, updates the software to the new version, and asks you to stop and restart the CES service.

Important:
- When you upgrade from a version prior to the CES 7.0.6547 March 2014 monthly release, an index data structure unmerge process will take place following the installation. The unmerge process will cause the index size to increase by about 5 to 10%. Ensure that your index drive offers sufficient free space before upgrading.
- You cannot install two Coveo instances of the same major version on a given server.
- Upgrading to a major release (such as from CES 6.5.4765 to 7.0.4784) is a migration process.

To upgrade CES on a Coveo server

1. Using an administrator account, connect to the Coveo back-end server on which you want to upgrade CES components.

   Important: When your Coveo deployment includes one or more Mirror servers, you must update the Master server first, and then update the Mirror server(s), repeating this procedure for each back-end server.

2. Ensure that the password of all users used by CES services (including the Diagnostic Tool) to log on are up to date. Otherwise, update the passwords in Windows Service Control Manager (see Configure How a Service Is Started).

3. From the email message that you receive from Coveo, download the appropriate CES installer (32-bit or 64-bit) for the new version. Contact Coveo Support if you need assistance to download the installer.

4. When you have a complex setup involving remote converters, prior to running the installer, proceed with the following requirements:
   - a. Disable the indexing process to pause the crawlers.
   - b. Switch the index to read-only mode to terminate on-going conversions properly.
   - c. Switch the index back to read-write mode.

5. Run the CES installer of the new CES version.

   Example: When CES 7.0.4781 is installed on the Coveo server, on a 64-bit server, use the Coveo Enterprise Search 7.0 x64 (4784).exe installer to install the CES 7.0.4784 version.

6. CES 7.0.6547+ (March 2014) When Microsoft .NET Framework 4.5 SP1 is not available on your server, a Coveo Enterprise Search 7 Setup dialog box appears. Click Install to download and install the missing Microsoft .NET Framework component.

   Important: The Microsoft .NET Framework installer will require that you restart the server following this installation when no prior Microsoft .NET Framework 4.5 version was installed on your server.
7. In the Welcome screen of the Coveo Enterprise Search 7.0 installer, click Next.

8. In the License Agreement screen, read the license terms, select I accept the terms in the license agreement, and then click Next.

9. When upgrading a Master server, in the Configuration screen, it is recommended and set by default to back up customized files (default folder: [CES_Path]\Backups):
a. Optionally, click **Configure**, and then in the **Backup Customized Files** screen:

![Backup Customized Files](image)

- i. Clear the **Backup customized files to the following folder** check box when you do not want to back up customized files.
- ii. Click **Change** to browse and select a different backup folder.
- iii. Click **OK**.

b. Click **Next**.

10. In the **Installing the program** screen, click **Install**.

   **Note**: If you get an error, ensure that the passwords of all users used by CES services (including the Diagnostic Tool) to log on are up to date before retrying the installation.

11. In the **Coveo Enterprise Search 7.0 (x64) Installation** dialog box, click **Yes** to continue the installation, acknowledging the fact that the CES service will be restarted if required.
A screen showing the installation progress bar appears.

12. In the installer **Installation Successful** screen, click **Finish**.

13. (For complex setups involving remote converters) Enable the indexing process to resume the crawlers.

### 3.5.12 About Coveo Platform Folders and Key Files

The following table identifies the three main folders where Coveo Platform files are installed. You can customize the base folders when you install the Coveo Enterprise Search components on Back-End servers and the Coveo .NET Front-End components on Front-End servers.

<table>
<thead>
<tr>
<th>Server</th>
<th>Folder description</th>
<th>Folder reference</th>
<th>Default path</th>
</tr>
</thead>
<tbody>
<tr>
<td>Back-End</td>
<td>CES installation folder</td>
<td>[CES_Path]</td>
<td>C:\Program Files\Coveo Enterprise Search 7</td>
</tr>
<tr>
<td>Back-End</td>
<td>Coveo index folder</td>
<td>[Index_Path]</td>
<td>C:\CES7</td>
</tr>
<tr>
<td>Front-End</td>
<td>.Net front-end installation</td>
<td>[.Net_Front-End_Path]</td>
<td>C:\Program Files\Coveo .NET Front-End 12</td>
</tr>
</tbody>
</table>

#### 3.5.12.1 Back-End CES Installation Folder and Files

**[CES_Path]**

This folder is the root folder for the CES binary and web files.

**Example:** The default path is `C:\Program Files\Coveo Enterprise Search 7\`

You can select a different path when you install CES (see "Installing CES on the Master Server" on page 28).
[CESPath]\Backups
This folder is created when you install a newer version or release of CES 7. For each upgrade, a subfolder is created using the current date and time (in the yyyy-mm-dd hh:mm format) and contains a backup of the [CESPath]\Instance folder.

[CESPath]\Bin
This folder contains all the CES binary files.

[CESPath]\CoreDumps
This folder is created when CES encounters a fatal error conditions. The complete CES process state is written to this folder to leave a trace of the issue context. These files can be used by the Coveo Support to diagnose the problem.

Note: The Coveo administrator can automatically receive an email alert message when a CES fatal error occurs.

[CESPath]\Installer
This folder contains the last CES installer used and the incremental installer patch file (.msp) applied to the current installed version. Do not delete or modify these files that are managed by the installer.

[CESPath]\Instance
This folder contains configuration files for this Coveo instance.

[CESPath]\Instance\License.txt
This text file contains the encrypted information describing the indexing capacity as well as optional features and modules that you purchased.

[CESPath]\Web\Admin
This folder contains all the Administration Tool files and subfolders.

[CESPath]\Web\Admin\Web.config
This file contains the basic Web server configuration for the Administration Tool.

3.5.12.2 Back-End Coveo Index Folder and Files

[IndexPath]
This folder contains the index and by default the associated files. You can change the default root folder (C:\CES7) and default subfolders for various associated files at the end of the installation process (see "Installing CES on the Master Server" on page 28). It is recommended to install the index on a dedicated hard disk drive (see "Index Size" on page 6).

Example: If D: is the dedicated hard disk drive, the index folder can be D:\CES7.

You can also move the index after it was created.
[Index_Path]\CertStore

This folder is the central store for the search security certificates used by the Coveo instance components to manage security.

[Index_Path]\Config

This folder contains the CES configuration files.

[Index_Path]\Config\Config.txt

This text file contains the CES configuration parameters that you can change from the Administration Tool.

**Important:** Do not directly edit this file unless explicitly instructed to do so by a Coveo Support agent.

**Note:** When you upgrade CES, the installer makes a backup copy of this file, adding the release number to the backup file name like Config-4757.txt.

[Index_Path]\Config\Config.bin

This file is the binary version of the CES configuration file (Config.txt) that is automatically created by CES. It must not be modified manually.

[Index_Path]\Config\Thesaurus.xml

This XML file contains the description of synonyms used to expand searches at query time. By default, this file contains no synonyms.

[Index_Path]\Index

This folder contains all the files and subfolders constituting the Coveo unified index.

[Index_Path]\Index\Default

This folder contains all the files and subfolders constituting the *default* mirror (see "Coveo Scalability Model" on page 14).

[Index_Path]\Index\Default\Default

This folder contains all the files and subfolders constituting the *default* slice (see "Coveo Scalability Model" on page 14).

[Index_Path]\Log

This folder contains all the Coveo index and system log files that you can review and manage from the Administration Tool.

[Index_Path]\Temp

This folder contains temporary cache files created and used by CES.
3.5.12.3 Front-End Folders and Files

[.Net_Front-End_Path]

This folder contains the Coveo .NET Front-End files.

**Example:** The default path is C:\Program Files\Coveo .NET Front-End 12

[.Net_Front-End_Path]Bin

This folder contains all the Coveo .NET Front-End binary files.

[.Net_Front-End_Path]Web

This folder contains all the files and subfolders for Coveo .NET Front-End search interfaces.

[.Net_Front-End_Path]Web\Web.config

This file contains the Web server configuration for .NET search interfaces.

[.Net_Front-End_Path]Web\*.aspx

These files are used as the default documents in IIS for the Coveo Enterprise Search website.

[.Net_Front-End_Path]Web\Coveo\Skins

This folder contains the subfolders for all the out-of-the-box and customized skins used by the Coveo .NET search interfaces.

[.Net_Front-End_Path]Web\SearchAdmin

This folder contains the .NET Interface Editor files and subfolders.

3.5.13 Extending CES Admin Service Certificate Validity Period

In a Coveo for Sitecore scenario, it is highly recommended to secure the CES Admin Service, thus ensuring only the authorized people perform administrative tasks on your CES instance using the service. For a connection to the service to be allowed, the application must provided access credentials as well as a certificate bounded to a specific port (443 by default). Past the certificate expiration date, all applications using the CES Admin Service stop working.

When installing (or upgrading to) CES 7.0.7814 or 7.0.8057 (August-December 2015), you can create a certificate valid for two years. This validity period cannot be modified, meaning that you must remind to generate a new certificate every two years for your Sitecore instance to work. If not, the following error will be thrown in the Coveo Diagnostic Page (see Troubleshooting Problems Using the Coveo Diagnostic Page):

```
System.Net.WebException: The underlying connection was closed: Could not establish trust relationship for the SSL/TLS secure channel. --
System.Security.Authentication.AuthenticationException: The remote certificate is invalid according to the validation procedure.
```
The solution is to generate a new certificate that lasts for 50 years using the installer of CES 7.0.8225+ (March 2016).

To extend the certificate validity period

1. Using an administrator account, connect to the Coveo Master server on which the CES Admin Service certificate is located.

2. From the email message that you receive from Coveo, download the appropriate CES installer (32-bit or 64-bit) for the March 2016 version or later. Contact Coveo Support if you need assistance to download the installer.

3. Run the CES installer.
   
   Example: When CES 7.0.8225 is installed on the Coveo server, on a 64-bit server, use the Coveo Enterprise Search 7.0 x64 (8225).exe installer to install the CES 7.0.8225 version.

4. In the Welcome screen of the Coveo Enterprise Search 7.0 installer, click Next.

5. In the License Agreement screen, read the license terms, select I accept the terms in the license agreement, and then click Next.

6. (When upgrading from CES 7.0.8047 (December 2015) only), in the Important information screen, click Next.

7. In the Configuration screen, next to Admin service security, click Configure.

8. In the next screen, click Choose next to the Change the user or certificate used to secure the Admin Service option.
9. In the **Coveo Enterprise Search Admin Service Security Options** screen:
a. If the default **Admin Service port number** (443) is used by another service or application, modify the port number.

b. Next to **Configure credentials for the Admin Service**, click **Configure**.
c. In the **Username**, **Password** and **Confirm Password** boxes, enter credentials that you create and take good note of them.

The specified username/password do not need to be that of an Active Directory or Sitecore user. They are encrypted and stored only on the Coveo server. These credentials will be used by application (such as the Coveo for Sitecore Search Provider) that need to authenticate to the Admin Service.

d. Click **OK**.

e. Next to **Configure a certificate for the Admin Service**, click **Configure**.
f. In the Create a certificate to secure the Admin Service screen, configure the certificate settings:

   Note: The certificate is valid for 50 years.

   i. In the CES Server name box, enter the fully qualified domain name (FQDN) of the CES server or an alias for future reference using your hosts file.

   Note: The default value is the computer name which often does not need to be modified.

   ii. In the Certificate private key password and Confirm password boxes, enter the password to protect the certificate private key.

   iii. When the default Admin Service port number (443) is used by another service or application, modify the port number.

   iv. Optionally click Browse to modify the default Certificate export path, which is the Coveo Enterprise Search 7 folder, and then click OK.

10. Back in the Coveo Enterprise Search Admin Service Security Options, click OK.

11. In the Configuration screen, click Next.

12. In the Installing the program screen, click Install.

13. In the Coveo Enterprise Search 7.0 (x64) Installation dialog box, click Yes to continue the installation,
acknowledging the fact that the CES service will be restarted if required.

![Coveo Enterprise Search 7.0 (x64) Installation](image)

**Note:** Restarting the CES Service and IIS typically takes less than a minute during which the CES service is unavailable to your end-users.

A screen showing the installation progress bar appears.

14. In the installer **Installation Successful** screen, click **Finish**.

### 3.5.14 Installing the Coveo Search API

The Coveo Search API implements a REST search endpoint that can be used by other Coveo products to communicate with your on-premises Coveo Enterprise Search (CES) index (see "Coveo REST Search API 8.0" on page 70). You can install the Coveo Search API on a server of your choice such as on the Coveo Master server (where Coveo Enterprise Search is installed), on a front-end server (where the Coveo JavaScript Search is installed), or any other server. Once installed, the Coveo Search API runs as a Windows service.

When your deployment includes one or more Coveo JavaScript Search interfaces, you must install and configure a Coveo Search API.

**Notes:**

- Coveo for Sitecore uses both the JavaScript Search and the Coveo Search API, but both are deployed by the Coveo for Sitecore installer (see **Installing Coveo for Sitecore**).
- You can also embed the Coveo Search API in ASP.NET or Java applications (see **Installation Options**).
- You can also install the Coveo Search API silently (see **Silent install**).

To install the Coveo Search API

1. Using an administrator account, connect to the server on which you decided to install the Coveo Search API.
2. **Download** the latest version of the Coveo Search API installer.
3. **Run** the Coveo Search API installer (**Coveo Search API 8.0.nnn.exe**).
4. When a previous version of the Search API was deployed with the ZIP file distribution and set as a Windows
service, you will see the following message. You need to stop and uninstall the old service (*Coveo REST Search API*) before you can continue this installation.

![Coveo Search API]

a. Click **OK**, and in the **Installation Cannot Proceed** screen, click **Finish**.

b. Open the Windows **Services** management console, and locate the **CoveoSsearchAPI** service.

c. In the folder where you extracted the Zip file, run the **Uninstall.bat** batch file.

d. Restart the Coveo Search API installer.

5. In the **Installation Folder** screen:

a. When the default installation folder is not appropriate (`C:\Program Files\Coveo Search API 8\`), select the desired folder.

b. When you are installing the Coveo Search API in the context of a Coveo for Sitecore deployment, select the **This installation is part of a Sitecore installation** check box.

c. Click **Next**.

6. If you selected the **This installation is part of a Sitecore installation** check box, in the **Application Secret Token** screen, click **Generate Random Token** to create an application secret token to be used by Coveo for Sitecore, and then click **Next**.

7. In the **Ready to Install** screen, click **Install**.

---

www.coveo.com
8. In the **Installation Successful** screen:
   
   a. When you are deploying a new install of the Coveo Search API and did not select the **This installation is part of a Sitecore installation** check box, the installer cannot start the Coveo Search API service.

   You must first edit the default configuration file to specify the Coveo server hosting the index (if not the localhost) and most probably to secure the access to the REST API.

   Click **Open config.yml** to edit the configuration file (by default C:\Program Files\Coveo Search API 8\config.yml) with a text editor of your choice (see "Customizing and Starting the Coveo Search API" on page 95).

   **Note:** You may need to set which application on your computer opens YAML files (.yml extension) by default. Choose a text editor such as Notepad.

   b. Click **Finish**.

   When you select the **This installation is part of a Sitecore installation** check box, the installer automatically configures and starts the Coveo Search API service.

To silently install Coveo Search API

(For advanced users only) The Coveo Search API installer can be launched in command line simply by calling the executable. Since the installer is made using Windows installer, msiexec options are supported, including /qn for a silent install (see Msiexec (command-line options)).

1. Using an administrator account, connect to the server on which you decided to install the Coveo Search API.

2. **Download** the latest version of the Coveo Search API installer.

3. Open **Command Prompt** as an administrator.

4. In **Command Prompt**:

   a. Using the **cd** command reach the Coveo Search API 8.0.nnn.exe file directory (see **Chdir (cd)**).

   b. Depending on the product for which you install the Search API:

   i. (For a Coveo product other than Coveo for Sitecore) Enter and execute the following command line where you replace nnn by the version number:

      "Coveo Search API 8.0.nnn.exe" /qn
Example: C:\Downloads\"Coveo Search API 8.0.802.exe" /qn

- (For Coveo for Sitecore)
  i. Generate a random string that will be used as the application secret.
  ii. Enter and execute the following command line in which you replace nnn by the version number and [value] by the application secret:

"Coveo Search API 8.0.nnn.exe" /qn APPLICATION_SECRET=[value]

Example: "Coveo Search API 8.0.802.exe" /qn APPLICATION_SECRET=123456789

Note: You also need to provide the application secret when installing the Coveo for Sitecore integration (see Installing Coveo for Sitecore).

3.5.14.1 Customizing and Starting the Coveo Search API

The Coveo Search API acts as is a bridge between the front-end search interfaces/applications and a Coveo Enterprise Search (CES) instance maintaining an index on the back-end (see "Coveo REST Search API 8.0" on page 70).

After installing a fresh copy of the Coveo Search API (see "Installing the Coveo Search API" on page 92) or when you want to modify how the service operates, you must edit the Coveo Search API configuration file.

The Coveo Search API configuration file:

- Is available in the root Coveo Search API folder, by default C:\Program Files\Coveo Search API 8\config.yml.
- Is in the YAML format, an easy to read data file format in which the indentation of the elements determines the data structure (see www.yaml.org).

Important: The indentation must be done by two spaces, not tabs. Using tabs will cause a syntax error and the service will immediately stop when you try to start it.

- Is made of various sections containing one or more parameters (see Windows Service Configuration File).

The default configuration file contains only a few of the possible sections and parameters to help you easily specify the index server and the common options to secure the API. The following procedure describes how to configure the common settings.

To customize and start the Coveo Search API

1. Using an administrator account, connect to the server on which the Coveo Search API is installed.

2. Using a text editor, open the [Search_API_Install_Path]\config.yml file (by default C:\Program Files\Coveo Search API 8\config.yml).

3. In the server section of the file:
Example: The Coveo Search API is installed on the same server as CES (myCoveoMasterServer) and uses the default port (52810).

<table>
<thead>
<tr>
<th>server:</th>
</tr>
</thead>
<tbody>
<tr>
<td>uri: <a href="https://myCoveoMasterServer:52810">https://myCoveoMasterServer:52810</a></td>
</tr>
<tr>
<td>serverCertificatePath: E:\CES70\Config\Certificates\cert-ca.pem</td>
</tr>
<tr>
<td>clientCertificatePath: E:\CES70\Config\Certificates\cert-iis.p12</td>
</tr>
</tbody>
</table>

a. For the uri parameter, enter the URI of your Coveo Master server (where Coveo Enterprise Search is installed) hosting the unified index with which you want this REST API to send query and receive search results.

When the Coveo Search API is on the same server as CES, the default uri (https://localhost:52810) will work.

When your Coveo Master server is not using the default service port (52810), enter the port it uses.

b. For the serverCertificatePath and clientCertificatePath parameters, enter the local path where respectively the CES server and client certificates can be found. The REST API will use these certificates to authenticate itself with the index server.

Note: When the Coveo Search API is on a different server than CES, you must copy the certificate files from the Coveo Master server (typically from the [Index_Path]\Config\Certificates\ folder to the path you enter on the server where the Coveo Search API is installed).

4. In the basicAuthentication, windowsAuthentication, and guest sections of the file, determine if and how users performing the search must be authenticated to be authorized to get results from the API:

Example: With this configuration, only Active Directory users can get results.

<table>
<thead>
<tr>
<th>basicAuthentication:</th>
</tr>
</thead>
<tbody>
<tr>
<td>enabled: false</td>
</tr>
<tr>
<td>provider: Active Directory</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>windowsAuthentication:</th>
</tr>
</thead>
<tbody>
<tr>
<td>enabled: true</td>
</tr>
<tr>
<td>provider: Active Directory</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>guest:</th>
</tr>
</thead>
<tbody>
<tr>
<td>enabled: false</td>
</tr>
<tr>
<td>name: DOMAIN\user</td>
</tr>
<tr>
<td>provider: Active Directory</td>
</tr>
</tbody>
</table>

a. For the enabled parameter, enter true when you want to enable this authentication mode.

Note: basicAuthentication passes credentials in clear text so it should always be used with secured HTTPS (SSL) connections or only for internal tests.

b. For the provider parameter, enter the name of the security provider that CES will use to validate the authentication.

Note: You can find the security provider name in the CES Administration Tool Security Providers page.
Example: When the API can be accessed publicly by anyone, you can enable the guest authentication mode for the S-1-1-0 Windows (Active Directory) Everyone well-known security identifier group.

```yaml
guest:
  enabled: true
  name: S-1-1-0
  provider: Active Directory
  type: Group
```

5. When one or more Web application will use this API, identify tokens/GUIDs that applications will need to provide to be authorized to use the API and that you will communicate only to trusted parties (see On-Premises Search Token Authentication):

Example: The search interfaces from your Web site and your Intranet use this API.

```yaml
tokens:
  sharedKey: a0534332-f093-4064-a712-4a79a97c9227

applications:
  - name: Website search
    secret: 353c7d37-7445-4217-a0ba-52c772c05632
    allowImpersonate: false
  - name: Intranet search
    secret: 8eSHODDPqGlMvqVY4v2wDut7sdRgwhovSQ1AWDLr1nTwSzJi2lDiK
    allowImpersonate: false
```

a. In the tokens section of the file, the sharedKey parameter needs to be set only in specific cases (see Configuring Search Token Generation). When this is the case, generate and enter a GUID to be used as a shared key token.

b. In the applications section of the file, create one subsection starting with a dash for each application that you want to authorize to use this API:

i. For the name parameter, enter a name of your choice that will identify the application. This name is only for your reference in this file.

ii. For the secret parameter, generate and enter a GUID to be used as the application secret token.

iii. For the allowImpersonate parameter, leave to false unless the application needs to perform search on behalf of someone else without having to supply the password.

Example: With Coveo for Salesforce, the user that performs a search is authenticated in Salesforce. The search application gets the user Salesforce account (email) and is set to impersonate this user to only return documents that this user has the permissions to see.

6. Save the file.

Note: You can add many other parameters to more specifically control how your Coveo Search API operates (see Windows Service Configuration File).

7. Start the Coveo Search API service:
a. Open the Windows Services management console.

b. Locate and right-click the Coveo Search API service, and then click Start.

c. Ensure that the service starts.

**Note:** The service immediately stops if the config.yml file contains a syntax error such as a tab character that is an invalid character in the YAML format (see REST Search API Windows Service Stops).

8. You can validate that the service is accessible from various computers:

a. Using a browser, access the URL in the following format:

   http://[REST_API_SERVER]:[port]/rest/search

   **Examples:**

   - From the same server when the port is the default (8080):
     http://localhost/rest/search
   - From another computer when the port is not the default:
     http://myRestApiServer:80/rest/search

b. Validate that the REST API JSON response appears in the browser.

### 3.6 Configuring Coveo Servers in a Network Load-Balancing Cluster

When your Coveo implementation includes two or more Front-End servers, it makes sense to somehow distribute the users towards the different servers. You can simply provide the address of each server only to a specific group of users.

A better practice is to define a network load-balancing (NLB) cluster for the Front-End servers, and provide the address of the cluster to all users. The load-balancer transparently and evenly distributes users on the available Front-End servers.

**Note:** You can use any third-party load-balancer product such as Microsoft Network Load-Balancing (see the Microsoft document Network Load Balancing Deployment Guide).

Similarly, when your Coveo implementation includes one or more Mirror servers, you probably want to distribute the query serving load among the Master and the available Mirror servers. Again, you can define a network load-balancing cluster for the Master server and the Mirror servers, and provide the address of the cluster to each Front-End server (see "Configuring .NET Front-End Server Query Destination" on page 102).
Two Coveo Front-End servers in a network load-balanced cluster
The Coveo Master server with two Mirror servers in another network load-balanced cluster
Coveo Master server with up to two slices
First Coveo Mirror server with copies of the Master server slices
Second Coveo Mirror server with copies of the Master server slices

Network load-balancing optimizes the usage of the Coveo Platform servers. It can also help ensuring high availability and failover capability in the event of planned or unplanned downtime for hardware, operating system, or application maintenance. With NLB clusters, scaling your Coveo implementation is also easier as you can transparently add Front-End or Mirror servers to the appropriate clusters.

**Tip:** When the Master server shows signs of process over load, with two or more Mirror servers, you can exclude the Master server from the NLB cluster to free the Master server from the query serving task.

**Note:** As an alternative solution to NLB, for Back-End servers, you can also consider using the failover alternate server feature (see "Configuring a .NET Front-End Server to Use Failover Alternate Back-End Servers" on page 100).
To configure Coveo Front-End servers in a network load-balancing cluster

1. Using a hardware or software load-balancer of your choice, create a NLB cluster that contains all the Coveo Front-End servers.

2. Setup a DNS name that points to this cluster.

3. Provide the Front-End cluster DNS name to your users to access the Coveo search interfaces.

To configure Coveo Back-End servers in a network load-balancing cluster

1. Using the hardware or software load balancer of your choice, create a NLB cluster that contains the Coveo Master server and the Mirror servers.

2. Setup a DNS name that points to this cluster.

3. Configure each Front-End server to send queries to the Back-End cluster DNS name (see "Configuring .NET Front-End Server Query Destination" on page 102).

3.7 Configuring a .NET Front-End Server to Use Failover Alternate Back-End Servers

Coveo .NET Front-End 12.0.74+ (February 2013)

A Coveo .NET Front-End server by default sends queries to a specific server originally selected during the Front-End first-time setup (see "Coveo .NET Front-End First Time Setup" on page 47). When your Coveo implementation includes one or more Mirror servers, to ensure continuous search service to end-users, you can configure a Front-End server to use one or more failover alternate servers when the default Back-End server is not responding.

Example: Your Coveo implementation includes two Front-End servers, one Master server, and two Mirror servers. You configure the Front-End 1 server to use the Mirror 1 server by default, but also to switch to the Mirror 2 or Master servers if the default server fails. Similarly, you configure the Front-End 2 server to use the Mirror 2 server by default but to switch to the Mirror 1 and Master as alternate servers.

The goal of the failover alternate server feature is to prevent showing Back-End server errors to end-users by redirecting their current action to the next responding server. When the default Back-End server stops responding, the currently active users experience a delay of a few seconds while the Front-End server confirms the server error and switches to the next available alternate server to resume the actions. The Front-End server monitors the non-responding Back-End server and transparently switches back to it when it starts responding.
**Note:** You cannot concurrently use the failover alternate server feature with network load-balancing (NLB) of Back-End servers. They are two exclusive server distribution management methods.

- Failover alternate server ensures a continuous service without errors but does not evenly distribute the load.
- NLB evenly distributes actions among multiple servers but generally does not trap exceptions so end-users can see Back-End server errors.

You can however use the failover alternate server feature with NLB configured to evenly distribute users among multiple Front-End servers (see "Configuring Coveo Servers in a Network Load-Balancing Cluster" on page 98).

To configure a .NET Front-End server to use failover alternate servers

1. Using a local administrator account, connect to the .NET Front-End server for which you want to configure failover alternate servers.

   **Note:** On a new Front-End server, ensure to perform the first-time Front-End setup before attempting to configure and enable the failover alternate server feature (see "Coveo .NET Front-End First Time Setup" on page 47).

2. Locate the web.config file of the IIS Web application hosting the Coveo .NET search interfaces.

   **Note:** When you chose to let the CES installer create the website, the default web.config file location is: [.NET_Front-End_Path]\Web\.

3. Using a text editor:
   a. Open the web.config file.

      **Note:** It is recommended to make a backup of the web.config file before editing it.

   b. As shown in the following code sample, under the <coveoEnterpriseSearch> tag, add an <alternateServers> section with one <add/> tag per alternate server:

   ```xml
   <coveoEnterpriseSearch>
   <server ... />
   <alternateServers enableFailover="true">
   <servers>
     <add id="" hostname="" port="" sslCertificatePath="" />
   </servers>
   </alternateServers>
   </coveoEnterpriseSearch>
   ```

   where the possible <alternateServers> tag attributes are:

   - enableFailover: Whether failover is enabled or not. The default value is false.
   - serversMonitoringDelayTimeSpan: The delay after which the Front-End server attempts to reconnect to unavailable Back-End servers. The default value is 5 seconds (00:00:05).
   - serversStopMonitoringTimeoutTimeSpan: The maximum amount of time to wait when stopping the server monitoring process. The default value is 5 seconds (00:00:05).
where the possible ```<add/>``` tag attributes are:

- **id**: The ID of your choice that uniquely identifies this CES mirror from the others.
- **hostname**: The hostname of the CES mirror computer.
- **port**: The port used to connect to the CES service on the mirror computer. The default value is 52800.
- **sslCertificatePath**: Optionally, the path to the SSL certificate used to connect to the CES mirror. When omitted, the sslCertificatePath of the main server is used.

**Note**: When more than one alternate server is configured, the Front-End server tries to use the first listed alternate server and relies on the second listed alternate server only when the first one is not responding, etc.

c. When your Coveo implementation includes more than one instance, to be able to see the Quick View for documents from remote indexes while failover alternate server is enabled, add the ```loadRemoteDocumentsFromMainServer="true"``` attribute to the ```<server>``` tag.

```xml
<coveoEnterpriseSearch>
  <server hostname="Mirror1" port="52800" loadRemoteDocumentsFromMainServer="true" />
  ...
</coveoEnterpriseSearch>
```

d. Save the file.

The changes take immediate effect for new actions.

4. Repeat this procedure for each Coveo Front-End Server.

**Note**: When Coveo is integrated like in SharePoint, modify the ```web.config``` file of each involved Web App on each SharePoint Front-End server.

### 3.8 Configuring .NET Front-End Server Query Destination

A Coveo .NET Front-End server by default sends queries to a specific server originally selected during the Front-End first-time setup (see "Coveo .NET Front-End First Time Setup" on page 47). You can manually change the target Coveo Back-End server from the ```web.config``` file of the IIS Web application.

#### To manually configure .NET Front-End server query destination

1. Using a local administrator account, connect to the Front-End server for which you want to change the query destination.

   **Note**: It is recommended to make a backup of the ```web.config``` file before editing it.

2. Locate the ```web.config``` file of the IIS Web application hosting the Coveo .NET search interfaces.

   **Note**: When you chose to let the CES installer create the website, the default ```web.config``` file location is: ```[.NET_Front-End_Path]\Web```.

3. Using a text editor:
a. Open the web.config file.

b. Locate the <coveoEnterpriseSearch> tag, and then set the value of the hostname attribute to the host name of the Coveo Back-End server to which you want this Front-End server to send queries by default.

Examples: Typical cases are:

- hostname="localhost" when the Front-End and Back-End components are on the same server.
- hostname="<CESMaster_hostname>" when the Front-End server sends queries to the Master server.
- hostname="<CESBackEndNLBCluster_DNS_name>" when the Front-End server sends queries to the DNS name of the NLB Back-End server cluster.

```
<coveoEnterpriseSearch>
  <server hostname="CESBackEndNLBCluster" port="52800" servicesHostname="CESBackEndNLBCluster" servicesPort="52810" instance="default" mirrorName="default" sslCertificatePath="C:\Program Files\Coveo .NET Front-End 12\Web\certificate.p12" />
</coveoEnterpriseSearch>
```

c. Save the file.

The changes take immediate effect for new queries.

4. Repeat this procedure for each Coveo .NET Front-End server.

3.9 Desktop Integration Package Deployment Overview

The Desktop Integration Package (DIP) installs the Desktop Searchbar and the Outlook Sidebar on end-user computers. The DIP can also allow end-users to configure which folders and files should be crawled from their computer to be added to the unified index.

Notes:

- The DIP works together with the Desktop connector to allow indexing of files stored on end-user computers. If it is not already done, before deploying the DIP, you must create and configure a Desktop connector source.
- The DIP can be deployed on Windows 8 or 7 end-user computers.
- With Outlook 2007 and up, for Windows systems, the outlook:// protocol used by the email result links in Coveo search interfaces (other than the Coveo Outlook Sidebar) is disabled by default. When you want users to be able to open email search results from these search interfaces directly in Outlook, if not already done, enable the protocol on all workstations for example using GPO (see Shortcuts and the Missing Outlook:// Protocol).
- The Desktop Integration Package currently does not support screen resolutions above 1920 x 1080 in which case the Outlook Sidebar appears too small.

The Desktop Searchbar and the Outlook Sidebar bring Coveo search a keystroke or a click away from where end-users work. These useful Coveo access points often help end-users to more quickly adopt the Coveo solution. The DIP is available to all Coveo implementations. For these reasons, it is recommended to deploy the DIP within your organization.

www.coveo.com
As a Coveo administrator, you need to download, distribute, install, and maintain updates of the Desktop Integration Package on the end-user desktop and laptop computers within your organization.

The following sections present the available DIP deployment methods.

**Group-Policy Object method**

In a Microsoft Windows Active Directory environment, this method consists in creating and configuring a Group Policy Object (GPO) to automatically manage the DIP distribution, installation, and updates on selected end-user computers (see "Creating a DIP Deployment Group Policy Object" on page 105).

This is the recommended method as it offers many advantages.

**Pros:**

- Controls exactly on which computer the DIP is installed.
- Controls which DIP features are enabled.
- Can pre-configure standard local folders to index.
- Automatically deploys the DIP initial version and updates.
- Contributes to maximize the usage and adoption of the Coveo solution.

**Cons:**

- Needs Active Directory environment and permissions.
- More complex configuration.

**Login script method**

This method consists in creating and using a login script to install the DIP when it is not already installed on the computer (see "Deploying the Desktop Integration Package Using a Login Script" on page 122).

**Pros:**

- Simple to configure
- Automatically deploys the DIP initial version.

**Cons:**

- Still need GPO if you want to control which DIP features are enabled.

**Manual distribution method**

This method consists in making the DIP installer available to your end-users and rely on them to install and configure the DIP (see "Manually Deploying the Desktop Integration Package" on page 122).

**Pros:**

- No configuration, only need to inform end-users of the availability of the DIP installer.

**Cons:**
Relies on end-user to install the DIP.

- Cannot control which DIP features are enabled.
- Each user must configure folders to index from scratch.
- Need to inform and rely on end-users to install updated version of the DIP.

What's Next?

Make DIP updates available for an easy deployment (see "Automatically Updating the DIP on All Computers" on page 123).

3.9.1 Creating a DIP Deployment Group Policy Object

In a Microsoft Windows Active Directory environment, the Group Policy Object (GPO) method allows you to centrally control how the Desktop Integration Package (DIP) is distributed, installed, updated, and initially configured on end-user computers. You can also decide which DIP features are available and configurable by end-users.

To create a DIP deployment GPO

1. Download the latest DIP version.

   **Note:** Ensure that you are currently using recent versions of CES and Coveo .NET Front-End (not necessary when deploying a Coveo Search API hosted JavaScript Search page) and consider upgrading to their latest version to prevent compatibility issues (see "Installing Coveo Platform Software Components" on page 25). Contact Coveo Support for more information.

2. Using an administrator account that meets the following requirements, connect to the domain server of your organization:
   - Permissions to create and edit group policies on the domain (at least a member of the Group Policy Creator and Owners).
   - Access to the Group Policy Management Console (GPMC)

3. Using the link provided by the Coveo support, download and save the DIP installer file (.exe or .msi) to a folder where all end-users for which you want to deploy the DIP have read and execute permissions.

   **Example:** Save the file in the [Your _DFS]\SysVol\[Your_Domain]\Policies folder.

4. You also need a copy of the DIP administrative template file on your server:
   a. Copy the content or download the administrative template file (see "Desktop Integration Package GPO Administrative Template File" on page 118).
   b. Save the file with the file name Coveo Desktop Integration Package Configuration.adm in a folder of your choice on the domain server.

5. Start the Group Policy Management Console (Start menu > Administrative Tools > Group Policy Management).

6. In the Group Policy Management console:
a. Open the organizational unit (OU) for which you want to add the DIP deployment GPO.

b. You can add the DIP deployment to an existing GPO or create a new one, in which case:
   
i. Right-click the organizational unit and select **Create and Link a GPO Here**.
   
   ii. In the **New GPO** dialog box, enter a name of your choice for the GPO, and then click **OK**.

   **Example:** Coveo Desktop Integration Package

c. Right-click on the newly created or existing GPO to which you want to add the DIP Deployment, and then select **Edit**.

7. In **Group Policy Object Editor** that appears:

a. In the tree, expand **User Configuration > Software Settings**.

b. Right-click **Software Installation**, and then select **New > Package**.

   ![Group Policy Object Editor](image)

   c. In the **Open** dialog box, select the DIP installer file (**Coveo Desktop Integration Package 12 EN.msi**) from the folder where you saved it, and then click **Open**.

   d. In the **Deploy Software** dialog box that appears, select **Assigned** to automatically install the DIP on end-user computers at logon, and then click **OK**.

   e. In the tree under **User Configuration**, right-click **Administrative Templates**, and then select **Add/Remove Templates**.

   f. In the **Add/Remove Templates** dialog box, click **Add**.
g. In the **Policy Templates** dialog box, select the DIP administrative template file that you saved on the domain server, and then click **Open**.

h. Back in the **Add/Remove Templates** dialog box, click **Close**.

What's Next?

Configure the DIP parameters in the Group Policy Object (see "Configuring the Desktop Integration Package GPO" on page 107).

3.9.1.1 Configuring the Desktop Integration Package GPO

In the Group Policy Object (GPO), you can configure three Desktop Integration Package (DIP) categories of parameters:

- General
- File Indexing
- Outlook Indexing

These categories correspond to the three tabs available to the end-user in the **Coveo Desktop Integration Package Options** dialog box.

In the GPO, you can specify the state of each parameter as:

**Not Configured**

The setting is not forced by the GPO and the end-user can change the corresponding parameters. The registry is not modified.

**Disabled**

Deactivates the setting. The end-user cannot change the corresponding parameters. The registry reflects that the policy setting is not selected.

**Enabled**

Activates the setting and allows to set a default value by GPO for the corresponding parameters. Depending on the parameter, the end-user can or cannot change the values. The registry reflects that the policy setting is selected.

To configure the Desktop Integration Package GPO

**Note:** This procedure is documented for a Windows Server 2008.

1. Connect to the domain server of your organization using an administrative account that meets the following requirements:
   - Permissions to create and edit group policies on the domain (at least a member of the Group Policy Creator and Owners).
   - Access to the Group Policy Management Console (GPMC).
2. Start the Group Policy Management Console (GPMC) (**Start menu > Administrative Tools > Group Policy**
3. In the **Group Policy Management** Console:
   
a. In the tree, expand **Group Policy Objects** in the forest and domain containing the GPO for the Desktop Integration Package.
   
b. Right-click the GPO for the Desktop Integration Package, and then click **Edit**.

4. In the **Group Policy Object Editor**:
   
a. Expand **User Configuration > Administrative Templates > Coveo Desktop Integration Package Configuration > General**.
   
b. In the **General** panel, in the **Setting** column, double-click **Set URI for the search page used**.

5. In the **Set URI for The Search Page Used** dialog box:
a. Select Enabled to set the Coveo Front-End server used by the Desktop Searchbar and the Outlook Sidebar. End-users will not be able to change the server.

   a. In the Search page URI parameter, enter the URI of the Coveo Front-End server.

   Example: https://MyCoveoServer.MyDomain.com

   Note: The GPO does not verify the format the entered URI. Ensure that the URI entered is valid.

b. Click Next Setting.

   Important: The URI of the Coveo Front-End server should be added to the trusted sites of the end-user Internet Explorer to prevent users from receiving frequent requests to authenticate themselves with their user name and password.

6. In the Allow Indexing on a Remote Server dialog box:
a. Select **Enabled** to force settings that end-users will not be able to change.

b. Select the **Index local documents and items on a remote server** check box.

   This enables indexing of the content from the desktop or laptop computer on which the DIP will be deployed.

c. Click **Show**, and in the **Show Contents** dialog box:
i. In the **Value** list, enter the address of the Coveo Back-End server in the `[hostname]:[port]` form. You can add more than one server. This is useful when you run separate instances of CES in two or more environments such as Development, Quality Assurance, and Production. You can specify the CES remote server name and port for each environment in which you want desktop/laptop indexed content to be sent.

**Note:** When no port is specified, the default value (1980) is used but it is strongly recommended to specify the port. The port must be the same value specified for the Desktop connector source.

ii. Click **OK**.

d. Click **Next Setting**.

7. In the **Show or Hide the Desktop Searchbar** dialog box:
a. Select **Enabled** to specify to either always show, never show, or hide the Desktop Searchbar.

b. Under **Options**, select only one of the following options:
   
   - **Always show the Desktop Searchbar**: The user will not be able to hide the Desktop Searchbar.
   - **Never show the Desktop Searchbar**: The user will never have access to the Desktop Searchbar.
   - **Hide the Desktop Searchbar by default**: The user will be able to show the Desktop Searchbar.

   c. Click **Next Setting**.

8. In the **Show or Hide the Outlook Sidebar** dialog box:
a. Select Enabled to specify to either always show, never show, or hide the Outlook Sidebar.

b. Under Options, select only one of the following options:

   - **Always show Outlook Sidebar**: The user will not be able to hide the Outlook sidebar.
   - **Never show Outlook Sidebar**: The user will never have access to the Outlook sidebar.
   - **Hide Outlook Sidebar by default**: The user will be able to show the Outlook sidebar.

c. Click OK.


10. In the File Indexing panel, in the Setting column, double-click Disable Remote File Indexing Override.

11. In the Disable Remote File Indexing Override dialog box, when you want that end-users cannot change the
local folders to index or to exclude from indexation:

![Image of the Disable Remote File Indexing Override dialog box]

a. Select **Enabled**.

b. Under **Options**, select the **Enable remote file indexing override** check box.

c. Click **Next Setting**.

12. In the **Define Local Folders To Index** dialog box:
a. Select Enabled to force a default list of folders to index.

b. Click Show.

c. In the Show Content dialog box, for each default local folder that you want to index, enter the folder full path, and then click OK.

d. Click Next Setting.

13. In the Define Local Folders to Exclude dialog box:
a. Select **Enabled** to force a default list of folders to exclude.

b. Click **Show**.

c. In the **Show Content** dialog box, for each default local folder that you want to exclude, enter the folder full path, and then click **OK**.

d. Click **OK**.

14. In the tree of the **Group Policy Object Editor**, expand **User Configuration** > **Administrative Templates** > **Coveo Desktop Integration Package Configuration** > **Outlook Indexing**.

15. In the **Outlook Indexing** panel, in the **Setting** column, double-click **Define PST Indexing Parameters**.

16. In the **Define PST Indexing Parameters** dialog box:
a. Select **Enabled** to set the default Outlook items to index by default.

b. Select the **Index the OST folder** check box to index the local Microsoft Exchange Offline Folders (.ost) mail archive files.

c. Select the **Index the PST folder** check box to index the local Microsoft Exchange Personal Folders (.pst) mail archive files.

d. Select the **Allow users to override PST indexing** check box when you selected the **Index the PST folder** check box but still want end-users to be able to disable it.

e. Click **Next Setting**.

17. In the **Define MAPI Profile Used for Indexing** dialog box, configure the default MAPI profile selection seen by the end-user:
Note: The MAPI profile parameter is useful only when a user has more than one Outlook profile and wants to index the content of a specific one. When it is not set, the content of the default profile is indexed.

a. Select Enabled to force a specific profile.

b. In the Use this MAPI profile box, enter the name of the MAPI profile to use.

c. Click OK.

3.9.1.2 Desktop Integration Package GPO Administrative Template File

This topic presents the content of the administrative template file (.adm) that you need when you deploy the Desktop Integration Package (DIP) using the Group Policy Object method (see “Creating a DIP Deployment Group Policy Object” on page 105).
; Coveo Desktop Integration Package Administrative Template File
;
; This file contains all the settings that are necessary to configure Group Policy
; settings for the Coveo Desktop Integration Package (DIP).
;
; Copyright (c) 2012 - Coveo Technologies Inc. - All Rights Reserved.
;
; ===========================================================================
;
; Current User Section
; ===========================================================================

CLASS USER

CATEGORY !!SearchBarCategory

;GENERAL TAB OPTIONS

;**************************************************************************

CATEGORY !!GeneralCategory

KEYNAME "software\policies\Coveo\Search Bar"

POLICY !!SearchPageUriPolicy

EXPLAIN !!SearchPageUri_Explain

PART !!SearchPageUri_EditText EDITTEXT REQUIRED

VALUENAME "SearchPageUri"

END PART

END POLICY

POLICY !!EnableRemoteIndexing_Policy

EXPLAIN !!EnableRemoteIndexing_Explain

PART !!EnableRemoteIndexing_CheckBox CHECKBOX

VALUENAME "EnableRemoteIndexing"

VALUEON NUMERIC 1

VALUEOFF NUMERIC 0

END PART

PART !!HostNamePort_Text TEXT

END PART

PART !!HostNamePort_EditText LISTBOX VALUEPREFIX "Host"

KEYNAME "software\policies\Coveo\Search Bar\RemoteIndexingServers\List"

END PART

END POLICY

POLICY !!ShowQuickSearchBar_Policy

EXPLAIN !!ShowQuickSearchBar_Explain

PART !!ShowQuickSearchBar_AlwaysShowCheckBox CHECKBOX

VALUENAME "AlwaysShowQuickSearchBar"

VALUEON NUMERIC 1

VALUEOFF NUMERIC 0

END PART

PART !!ShowQuickSearchBar.NeverShowCheckBox CHECKBOX

VALUENAME "NeverShowQuickSearchBar"

VALUEON NUMERIC 1

VALUEOFF NUMERIC 0

END PART

PART !!ShowQuickSearchBar.HideByDefault CHECKBOX

VALUENAME "HideQuickSearchBarByDefault"

VALUEON NUMERIC 1

VALUEOFF NUMERIC 0

END PART

END POLICY

POLICY !!ShowSideBar_Policy

EXPLAIN !!ShowSideBar_Explain

PART !!ShowSideBar_AlwaysShowCheckBox CHECKBOX

VALUENAME "AlwaysShowOutlookSideBar"

VALUEON NUMERIC 1

VALUEOFF NUMERIC 0

END PART

END POLICY


VALUENAME "NeverShowOutlookSideBar"
VALUE ON NUMERIC 1
VALUE OFF NUMERIC 0
END PART
PART !!ShowSideBar_HideByDefault CHECKBOX
VALUENAME "HideOutlookSideBarByDefault"
VALUE ON NUMERIC 1
VALUE OFF NUMERIC 0
END PART
END POLICY
END CATEGORY

;*****************************************************************
;FILESYSTEM TAB OPTIONS
;*****************************************************************
CATEGORY !!FilesystemCategory
POLICY !!DisableRemoteFileIndexing_Policy
KEYNAME "software\policies\Coveo\Search Bar"
EXPLAIN !!DisableRemoteFileIndexing_Explain
PART !!DisableRemoteFileIndexing_ChoiceBox CHECKBOX
VALUENAME "DisableRemoteFileIndexing"
VALUE ON NUMERIC 1
VALUE OFF NUMERIC 0
END PART
END POLICY
END CATEGORY

POLICY !!FoldersToIndex_Policy
KEYNAME "software\policies\Coveo\Search Bar\FoldersToIndex\List"
EXPLAIN !!FoldersToIndex_Explain
PART !!FoldersToIndex_ListBox LISTBOX VALUEPREFIX "Path"
END PART
END POLICY
END CATEGORY

POLICY !!ExcludedFolders_Policy
KEYNAME "software\policies\Coveo\Search Bar\ExcludedFolders\List"
EXPLAIN !!ExcludedFolders_Explain
PART !!ExcludedFolders_ListBox LISTBOX VALUEPREFIX "Path"
END PART
END POLICY
END CATEGORY

;OUTLOOK TAB OPTIONS
;*****************************************************************
CATEGORY !!OutlookCategory
KEYNAME "software\policies\Coveo\Search Bar"

POLICY !!OutlookItemsToIndex_Policy
EXPLAIN !!OutlookItemsToIndex_Explain
PART !!IndexExchangeStore_ChoiceBox CHECKBOX
VALUENAME "IndexExchangeStore"
VALUE ON NUMERIC 1
VALUE OFF NUMERIC 0
END PART
PART !!IndexMAPIOnlineStores_ChoiceBox CHECKBOX
VALUENAME "IndexMAPIOnlineStores"
VALUE ON NUMERIC 1
VALUE OFF NUMERIC 0
END PART
PART !!UserCanChangeIndexMAPIOnlineStores_ChoiceBox CHECKBOX
VALUENAME "UserCanOverrideIndexMAPIOnlineStores"
VALUE ON NUMERIC 1
VALUE OFF NUMERIC 0
END PART
END POLICY
END CATEGORY

POLICY !!MAPIProfileName_Policy
EXPLAIN !!MAPIProfileName_Explain
PART !!MAPIProfileName_EditText EDITTEXT REQUIRED
VALUENAME "MAPIProfileName"
END PART
END POLICY
END CATEGORY
END CATEGORY

Strings

[Strings]
SearchBarCategory="Coveo Desktop Integration Package configuration"

GeneralCategory="General"

SearchPageUrlPolicy="Set URI for the Search Page Used"
SearchPageUrlExplain="Enabling this policy and setting it to a URI defines the search page that will be used."
SearchPageUrlEditText="Search page URI:"

EnableRemoteIndexingPolicy="Allow Indexing on a Remote Server"
EnableRemoteIndexingExplain="This policy allows the indexing of desktop or laptop computer content on one or more remote servers. When this policy is enabled, you must specify at least one remote server using the hostname:port form. When no port is specified, the default port (1980) is used. The port must be the same as the one used by the Desktop connector."
EnableRemoteIndexingCheckBox="Index local documents and items on a remote server"
HostNamePortText="Specify servers using the hostname:port form."
HostNamePortEditText="Set remote server name and port:"

ShowQuickSearchBarPolicy="Show or Hide the Desktop Searchbar"
ShowQuickSearchBarExplain="Enabling this policy allows specifying whether the Desktop Searchbar is visible or not."
ShowQuickSearchBarAlwaysShowCheckBox="Always show the Desktop Searchbar"
ShowQuickSearchBarNeverShowCheckBox="Never show the Desktop Searchbar"
ShowQuickSearchBarHideByDefault="Hide Desktop Searchbar by default"

SidebarCategory="File Indexing"

DisableRemoteFileIndexingPolicy="Disable Remote File Indexing Override"
DisableRemoteFileIndexingExplain="Enabling this policy prevents end-users from changing the folders to index and the excluded folders."
DisableRemoteFileIndexingCheckBox="Disable remote file indexing override"

FoldersToIndexPolicy="Define Local Folders to Index"
FoldersToIndexExplain="This policy contains the list of folders to index."
FoldersToListBox="Local folders to index:"

ExcludedFoldersPolicy="Define Local Folders to Exclude"
ExcludedFoldersExplain="This policy contains the list of folders to exclude from indexing."
ExcludedFoldersListBox="Folders to exclude:"

OutlookCategory="Outlook Indexing"

OutlookItemsToIndexPolicy="Define PST Indexing Parameters"
OutlookItemsToIndexExplain="This policy defines the Outlook folders to index."
IndexExchangeStoreCheckBox="Index the OST folder"
IndexMAPIServerOnlineStoresCheckBox="Index the PST folder"
UserCanChangeIndexMAPIServerOnlineStoresCheckBox="Allow users to override PST indexing"

MAPIProfileNamePolicy="Define MAPI Profile Used for Indexing"
MAPIProfileNameExplain="Enabling this policy allows to specify the MAPI profile to use for indexing user's PST and OST folders."
MAPIProfileNameEditText="Use this MAPI profile:"
3.9.2 Deploying the Desktop Integration Package Using a Login Script

The login script method for the Desktop Integration Package (DIP) deployment consists in creating a login script that starts the DIP installer when it detects that the DIP is not already installed on the end-user computer on which a user logs in.

**Note:** You can still use GPO to remotely set the DIP configuration for all users.

To deploy the DIP using a login script

1. Download the latest DIP version.

   **Note:** Ensure that you are currently using recent versions of CES and Coveo .NET Front-End and consider upgrading to their latest version to prevent compatibility issues (see "Installing Coveo Platform Software Components" on page 25). Contact Coveo Support for more information.

2. Copy the DIP installer to a network location available from a login script for all users.

3. Using a text editor:

   a. Create a login script that starts the DIP installer only when the DIP is not already installed on the computer using the following commands:

   ```batch
   REM DETECT IF THE PACKAGE IS ALREADY INSTALLED ON WINDOWS XP
   IF exist "%Userprofile%\Local Settings\Application Data\Coveo\Coveo Desktop Integration Package\Extensibility.dll" goto END
   REM DETECT IF ALREADY INSTALLED ON WINDOWS VISTA AND WINDOWS 7
   IF exist "%LOCALAPPDATA%\Local\Coveo\Coveo Desktop Integration Package\Extensibility.dll" goto END
   "[path]\Coveo Desktop Integration Package.exe"
   :END
   ```

   where you replace `[path]` (in the last line before :END) by the path where you saved the DIP installer.

   **Note:** You can use the .exe installer file with the /nocloseapplications command line to update the DIP without requiring Outlook to be closed and restarted.

   b. Save the file with a .bat extension in the folder that corresponds to the domain controller's Netlogon shared folder.

3.9.3 Manually Deploying the Desktop Integration Package

The manual method for the Desktop Integration Package (DIP) deployment simply consists in making the DIP installer available to your end-users and relies on them to install and configure the DIP.

**Note:** With this method, all DIP features are enabled to all end-users. You cannot enable/disable or pre-configure folders to index as you can do with the GPO method.
To manually deploy the DIP

1. **Download the latest DIP version.**

   Note: Ensure that you are currently using recent versions of CES and Coveo .NET Front-End and consider upgrading to their latest version to prevent compatibility issues (see "Installing Coveo Platform Software Components" on page 25). Contact Coveo Support for more information.

2. Save the DIP installer to a location available to all your end-users.

3. Inform your end-users of the availability of the DIP installer and provide instructions to install and configure the DIP.

3.9.4 Automatically Updating the DIP on All Computers

The Desktop Integration Package (DIP) comes with a built-in feature that periodically checks for available DIP updates. All you have to do is copy the new DIP installer file to a specific location on the Coveo .NET Front-End server with which the DIP communicates. The DIP does the rest.

Note: Desktop Integration Package 12.0.1840+ (June 2016) If you use a JavaScript user interface (e.g., the search page that comes with the Coveo Search API install kit) in the DIP, when a new DIP version will become available, ask your IT department to overwrite the DIP install kit in the file share folder to which the GPO is referring, and force a GPO update to update the DIP on your user machines.

Here is how it works:

- A user starts the DIP (it typically starts automatically after starting Windows).
- One minute after starting, and every four hours while running, the DIP checks for the availability of a new DIP installer version at the following URL:

  http://[FrontEndServer]/coveo/anonymous/searchbar/Coveo Desktop Integration Package.exe

  where [FrontEndServer] is the server defined in the URL of the search page box for the DIP configuration.
- When a new installer version is available, the DIP automatically starts the installer and the user sees a Coveo Desktop Integration Package Update dialog box.

- The user can decide to perform the update immediately or cancel it, in which case the dialog box will appear again every four hours while the DIP is running.

With this mechanism, all active DIP users will be offered to update within a few hours.
To automatically update the DIP

**Important:** This procedure only applies when you integrated a Coveo .NET Front-End search page in the DIP. You must ask your IT department to create a GPO to automatically update a DIP integrated with a Coveo JavaScript Search page.

1. Using an administrator account, connect to the Coveo .NET Front-End server from which the DIP gets search results. This is the server defined in the **URL of the search page** box for the DIP configuration.

2. **Download the latest DIP version.**

   **Note:** Ensure that you are currently using recent versions of CES and Coveo .NET Front-End and consider upgrading to their latest version to prevent compatibility issues (see "Installing Coveo Platform Software Components" on page 25). Contact Coveo Support for more information.

3. **Copy the new Coveo Desktop Integration Package.exe file** in the following folder (replacing an older one if it was there):

   C:\Program Files\Coveo .NET Front-End 12\Web\Coveo\Anonymous\SearchBar

   The installer file in this folder corresponds to the following URL:

   http://[FrontEndServer]/coveo/anonymous/searchbar/Coveo Desktop Integration Package.exe

4. On a computer on which the DIP is installed, start the DIP to test that you get the **Coveo Desktop Integration Package Update** dialog box.

3.10 Deploying the .NET Search Interface URL Shortener Database

The Coveo .NET Front-Ends can optionally use a MongoDB database to manage shortened URLs (see "About the .NET Search Interface URL Shortener" on page 125). MongoDB is an easy to set up, free, scalable, high-performance, open source, NoSQL database that supports replication and high availability.

You can install MongoDB on any server that is accessible to your Coveo .NET Front-End server(s). MongoDB and its usage by the Coveo Platform require low computer resources.

**Examples:**

- In the case of a one server Coveo instance, installing MongoDB on the Coveo server is the simplest solution.

- In the case of a Coveo instance with multiple Coveo .NET Front-End servers, you could choose to install MongoDB on the Coveo Master server, on one of the Coveo Front-End server, or on another server.

To deploy the URL shortener database

1. **Install MongoDB on a server of your choice** (see "Installing MongoDB on a Server" on page 125).

   **Note:** You can achieve MongoDB high availability by installing MongoDB on three or more servers and configure a replica set (see the MongoDB document [Replica Sets - Basics]).
2. On each Coveo Front-End server, activate the URL shortener (see “Enabling the URL Shortener Database” on page 128).

3.10.1 About the .NET Search Interface URL Shortener

Coveo .NET Front-End servers use the URL to exchange search interface parameters with the Coveo Back-End server. When several search parameters are needed, the number of characters in the URL increases.

**Example:** Dashboards such as Case Consoles or Account Consoles can produce very long URLs.

A long URL becomes a problem when it exceeds the 2083-character URL length limit of Internet Explorer. The browser truncates longer URLs, causing various types of errors.

The Coveo .NET Front-End servers support a URL shortener feature that overcomes this problem. The URL shortener stores the original URL parameters in a database, and rather passes a 24-character alphanumeric reference string to the browser.

**Example:** A more than 2083-character long original URL is reduced to the following shortened URL:

http://localhost:8080/#s=4f4d03636e92f50a8ceebe8f

A shorter URL is also more elegant to share and can be included in a Tweet.

The Coveo .NET Search Interface URL shortener feature requirements are:

- Front-End servers must have access to a MongoDB database where the shortened URLs are stored (see "Installing MongoDB on a Server" on page 125).
- On each Coveo .NET Front-End server, you must configure and enable the URL shortener feature (see "Enabling the URL Shortener Database" on page 128).

3.10.2 Installing MongoDB on a Server

Your Coveo instance must have access to a MongoDB database when you want to enable the URL shortener feature (see "About the .NET Search Interface URL Shortener" on page 125).

MongoDB supports basic authentication allowing you to secure the access to the database. Unless you install MongoDB in a secured environment, it is recommended to activate the MongoDB authentication and create and connect with a MongoDB user that has read and write permissions to the database.

**Note:** When you choose to use user-based security, you must include the username and password in the connection string (see "Enabling the URL Shortener Database" on page 128). As described in the following procedure, you enable the MongoDB authentication by including the --auth option when you register the MongoDB service.

To install MongoDB on a server

1. Using an administrator account, connect to the server on which you want to install MongoDB as a Windows service.

2. Download the latest production release of MongoDB for Windows (see the MongoDB document [MongoDB](https://www.mongodb.com/documentation)).
3. Unzip the downloaded binary package to the location of your choice.

Example: Unzip to C:\Program Files\mongodb-win32-x86_64-2.0.2 and rename to C:\Program Files\mongodb to have a version-independent folder name.

4. Create the folder where MongoDB will store data:
   - Create the default folder [Same_Drive]\data\db.
     Example: C:\data\db
   - OR
   - Create a custom folder of your choice, in which case you must use the --dbpath option to specify the database folder when you register the MongoDB service.
     Example: Create the D:\MongoDB\folder.

5. When you choose to enable the MongoDB authentication, create one or more MongoDB users that you will use to access one or more databases:

   Note: A MongoDB user has read and write permissions to the database to which it is added.

   a. Start the MongoDB interactive shell, by running the [MongoDB_Path]\bin\mongo.exe file.
      Example: Using Windows explorer, double-click the C:\Program Files\mongodb\bin\mongo.exe file.
   
   b. In the MongoDB interactive shell, if not already done, first switch to the admin database and create an administrator account.
      Example: To switch to the admin database and create an administrator user named admin with the password adminpassword, type the following commands:
      > use admin  
      > db.addUser("admin", "adminpassword")
   
   c. If not already authenticated, login as the administrator.
      Example:
      > db.auth("admin", "adminpassword")
   
   d. Create the normal user for a new or existing database to be used by the Coveo Platform.
Example: To create the URLShortener database and create a normal user named MyCoveoUser with the password MyPassword for this database, type the following commands:

```plaintext
> use URLShortener
> db.addUser("MyCoveoUser", "MyPassword")
```

Note: Refer to the MongoDB documentation when you need more information on the authentication (see the MongoDB document Configuring Authentication and Security).

6. Register the MongoDB as a Windows service:
   a. Open a command line prompt (on the Windows taskbar, select Start, type cmd, and then press enter).
   b. Change directory to the MongoDB installation folder.
      
      Example: In the command line prompt, enter: `cd \Program Files\MongoDB\bin`
   c. Enter the following command:

```
mongod --install --serviceName "MongoDB" --dbpath [MongoDB_Folder] --logpath [MongoDB_Log_File] --auth
```

   where:

   - you include the `--dbpath` option when you want to use a database folder other than the default one. Replace `[MongoDB_Folder]` by the desired path where MongoDB automatically creates the databases.
   - you include the `--logpath` option when you want to record MongoDB messages in a log file. Replace `[MongoDB_Log_File]` by the desired path and file name that MongoDB creates automatically. When omitted, MongoDB sends messages to the standard output (stdout).
   - you include the `--auth` option when you want to enable user authentication, restricting access only to users defined in MongoDB.

   Note: You must add at least one user from the interactive shell on the localhost before starting the server with authentication. You cannot add the first user from a connection that is not local with respect to mongod.

Example: The following command registers MongoDB as a Windows service that will accept connections only for authenticated users:

```
mongod --install --serviceName "MongoDB" --dbpath D:\MongoDB --logpath D:\MongoDB\MongoDB.log --auth
```

7. Still in the command line prompt, start the service by typing the following command:

```
net start MongoDB
```

Note: The MongoDB service will start automatically on future server startups.
What's Next?

Enable the desired optional database features (see "Enabling the URL Shortener Database" on page 128).

3.10.3 Enabling the URL Shortener Database

Once MongoDB is installed on a server accessible to a Coveo .NET Front-End server (see "Installing MongoDB on a Server" on page 125), you can activate the URL shortener.

In the case of a Coveo instance with multiple Front-End servers, you must perform the following procedure on each Front-End server.

To enable the URL shortener databases on a Coveo .NET Front-End server

1. Using an administrator account, connect to the Coveo .NET Front-End server.

2. Using a text editor:
   a. Open the [.NET_Front-End_Path]\Web\Web.config file.

   Example: By default: C:\Program Files\Coveo .NET Front-End 12\Web\Web.config

   b. In the <coveoEnterpriseSearch> section of the file, edit the following line to enable the URL shortener database feature:

   ```xml
   <database enabled="true" connectionString="mongodb://[username:password@]([MongoDB_Server]/[databaseName])"/>
   ```

   where:
   - you include the [username:password@] prefix when you enabled authentication. Replace [username:password@] by the credentials of a user with read and write permissions to this database.
   - you replace [MongoDB_Server] with the hostname of the MongoDB server.
   - you replace [databaseName] with the name that you want to use for the database. MongoDB automatically creates a database using the name that you provide if it does not already exist. If you already created the database and users, ensure to use the same database name.

   Examples: When MongoDB is available from this Coveo .NET Front-End server:

   ```xml
   <database enabled="true" connectionString="mongodb://localhost/SearchInterfaceInfo"/>
   ```

   When MongoDB is available from the MyMongoDBServer server and authentication is enabled:

   ```xml
   <database enabled="true" connectionString="mongodb://MyCoveoUser:MyPassword@MyMongoDBServer/SearchInterfaceInfo"/>
   ```

   c. Save the file.

   The features are immediately effective on this Coveo .NET Front-End server.
3.11 Enabling a User Profile Database

A Coveo .NET Front-End user profile contains the end-user preferences, saved queries, and saved filters.

You can use MongoDB to allow the Coveo .NET Front-End to save user profiles in a database rather than in browser cookies. Search users can then access their personal profile from any browser on any device even in environments where browser cookies are not allowed or deleted manually or automatically.

To enable a profile database on a Coveo .NET Front-End server

1. Install MongoDB on a server accessible to your Coveo .NET Front-End server (see "Installing MongoDB on a Server" on page 125).

2. Using an administrator account, connect to your Coveo .NET Front-End server.

3. Using a text editor:
   a. Open the [.NET_Front-End Path]\Web.config file.

   Example: By default: C:\Program Files\Coveo .NET Front-End 12\Web\Web.config

   b. In the <coveoEnterpriseSearch> section of the file, edit the following line to enable the user profile database feature:

   
   ```xml
   <database enabled="true" userProfileConnectionString="mongodb://[username:password@][MongoDB_Server]/[databaseName]"/>
   ```

   where:
   - you include the [username:password@] prefix when you enabled authentication. Replace [username:password@] by the credentials of a user with read and write permissions to this database.
   - you replace [MongoDB_Server] with the hostname of the MongoDB server.
   - you replace [databaseName] with the name that you want to use for the database. MongoDB automatically creates a database using the name that you provide if it does not already exist. If you already created the database and users, ensure to use the same database name.

   Example: When MongoDB is available from the MyMongoDBServer server and authentication is enabled:

   ```xml
   <database enabled="true" userProfileConnectionString="mongodb://MyCoveoUser:MyPassword@MyMongoDBServer/UserProfile"/>
   ```

   c. Save the file.

   The features are immediately effective on this Coveo .NET Front-End server.

4. In the case of a Coveo instance with multiple Front-End servers, repeat this procedure on all other Front-End servers.
3.12 Creating a Custom Color Scheme for the Desktop Searchbar in the Windows Registry

Deprecation

Desktop Integration Package 12.0.316+ (October 2013)

End-users can select an out-of-the-box predefined color scheme for the Desktop Searchbar. It is also possible to create a custom color scheme for the Desktop Searchbar, for example to match your organization official colors.

Note: Desktop Integration Package 12.0.1888+ (September 2016) You can create custom color schemes in a JSON file stored on the web server from which the DIP gets results, without requiring your end-users to create registry keys on their machine.

For search interfaces powered by Coveo .NET Front-End, create and refer to the file containing the color schemes in the DIP JSON configuration file (see Customizing Desktop Integration Package (DIP) Bitmaps and Colors).

To create a custom color scheme for the Desktop Searchbar in the Windows registry

1. Log in to a computer on which the Desktop Integration Package is installed.
2. Turn off the Desktop Integration Package by selecting the contextual menu of the Coveo Desktop Integration Package system icon, and then selecting Exit in the contextual menu.
3. Open the Windows Registry Editor (by pressing the Windows+r keys, and then typing regedit).
4. In the Registry Editor:
   a. Search or navigate to HKEY_CURRENT_USER > Software > Coveo > Search Bar > SearchBarScheme.
   b. Right-click SearchBarScheme, and then select New > Key.
   c. In the new folder, enter a name for your new color scheme. This name however is not the color scheme name that the end-user will see.
   d. Right-click the new folder, select New > String Value, and create each of the string values described in the following table.

Tip: You can start with colors from one of the out-of-the-box color schemes (see "Default Desktop Searchbar Color Schemes" on page 171).
5. Restart the DIP by selecting the Windows Start button, typing Coveo Search Bar, and then pressing Enter.

6. From the DIP options, select the newly created color scheme.

7. Validate that the scheme appears as expected.

3.12.1 Default Desktop Searchbar Color Schemes

The following table presents the Registry Editor values for the default HKEY_CURRENT_USER > Software > Coveo > Search Bar > SearchBarScheme Desktop Searchbar color schemes (see "Creating a Custom Color Scheme for the Desktop Searchbar in the Windows Registry" on page 169).

<table>
<thead>
<tr>
<th>Registry string name</th>
<th>Black</th>
<th>Light blue</th>
<th>Blue</th>
<th>Light gray</th>
<th>Gray</th>
<th>Light orange</th>
<th>Orange</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Registry string name</td>
<td>Black</td>
<td>Light blue</td>
<td>Blue</td>
<td>Light gray</td>
<td>Gray</td>
<td>Light orange</td>
<td>Orange</td>
</tr>
<tr>
<td>-----------------------------------------</td>
<td>-------</td>
<td>------------</td>
<td>-------</td>
<td>------------</td>
<td>-------</td>
<td>--------------</td>
<td>--------</td>
</tr>
<tr>
<td>Name</td>
<td>Black</td>
<td>Light Blue</td>
<td>Blue</td>
<td>Light gray</td>
<td>Gray</td>
<td>Light orange</td>
<td>Orange</td>
</tr>
<tr>
<td>SearchbarBackgroundColorResultColor</td>
<td>#C8C8</td>
<td>#F3F3F</td>
<td>#CFDDE</td>
<td>#F3F3F</td>
<td>#DAEE</td>
<td>#FFCA9</td>
<td></td>
</tr>
<tr>
<td>SearchbarBackgroundColorSearchColor</td>
<td>#E1E1</td>
<td>#EBF5F</td>
<td>#E7F1F</td>
<td>#E2E2E</td>
<td>#DAEE</td>
<td>#FEF0E</td>
<td></td>
</tr>
<tr>
<td>SearchbarCloseButtonBorderColor</td>
<td>#ABABA</td>
<td>#ABABA</td>
<td>#ABABA</td>
<td>#ABABA</td>
<td>#ABABA</td>
<td>#ABABA</td>
<td></td>
</tr>
<tr>
<td>SearchbarInterfaceLabelColor</td>
<td>#F3F3F</td>
<td>#F3F3F</td>
<td>#F3F3F</td>
<td>#F3F3F</td>
<td>#F3F3F</td>
<td>#F3F3F</td>
<td></td>
</tr>
<tr>
<td>SearchbarSearchButtonOverColor</td>
<td>#F68D3</td>
<td>#F68D3</td>
<td>#F68D3</td>
<td>#F68D3</td>
<td>#F68D3</td>
<td>#F68D3</td>
<td></td>
</tr>
<tr>
<td>SearchbarFormBorderColor</td>
<td>#ABABA</td>
<td>#ABABA</td>
<td>#8BA0B</td>
<td>#ABABA</td>
<td>#A5ACB</td>
<td>#ABABA</td>
<td>#F4802</td>
</tr>
<tr>
<td>SearchbarSearchTextboxBorderColor</td>
<td>#BDBDB</td>
<td>#BDBDB</td>
<td>#BDBDB</td>
<td>#BDBDB</td>
<td>#BDBDB</td>
<td>#BDBDB</td>
<td></td>
</tr>
<tr>
<td>SearchbarUndockButtonBorderColor</td>
<td>#ABABA</td>
<td>#ABABA</td>
<td>#ABABA</td>
<td>#ABABA</td>
<td>#ABABA</td>
<td>#ABABA</td>
<td></td>
</tr>
<tr>
<td>SearchButtonBorderColor</td>
<td>#D36C0</td>
<td>#D36C0</td>
<td>#D36C0</td>
<td>#D36C0</td>
<td>#D36C0</td>
<td>#D36C0</td>
<td></td>
</tr>
<tr>
<td>SearchButtonColor</td>
<td>#F47F2</td>
<td>#F47F2</td>
<td>#F47F2</td>
<td>#F47F2</td>
<td>#F47F2</td>
<td>#F47F2</td>
<td></td>
</tr>
</tbody>
</table>

### 3.13 Creating a Custom Color Scheme for the Outlook Sidebar in the Windows Registry

**Deprecated**

**Desktop Integration Package 12.0.316+ (October 2013)**

End-users can select an out-of-the-box predefined color scheme for the Outlook Sidebar. It is also possible to create a custom color scheme for the Outlook Sidebar, for example to match your organization official colors.
Note: Desktop Integration Package 12.0.1888+ (September 2016). You can create custom color schemes in a JSON file stored on the web server from which the DIP gets results, without requiring your end-users to create registry keys on their machine.

For search interfaces powered by Coveo .NET Front-End, create and refer to the file containing the color schemes in the DIP JSON configuration file (see Customizing Desktop Integration Package (DIP) Bitmaps and Colors).

To create a custom color scheme for the Outlook Sidebar in the Windows registry

1. Log in to a computer on which the Desktop Integration Package is installed.
2. Close Outlook.
3. Turn off the Desktop Integration Package by selecting the contextual menu of the Coveo Desktop Integration Package system icon ⚙, and then selecting Exit in the contextual menu.
4. Open the Windows Registry Editor (by pressing the Windows+r keys, and then typing regedit).
5. In the Registry Editor:
   a. Search or navigate to HKEY_CURRENT_USER > Software > Coveo > Search Bar > OutlookScheme.
   b. Right-click OutlookScheme, and then select New > Key.
   c. For the new folder, enter a name for your new color scheme. This name however is not the color scheme name that the end-user will see.
   d. Right-click the new folder, select New > String Value, and create each of the string values described in the following table.

<table>
<thead>
<tr>
<th>Name</th>
<th>Value (example)</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default</td>
<td>0</td>
<td>Set to 1 to make this scheme the default scheme.</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Important:</strong> Only one scheme must be the default theme otherwise the DIP will not start.</td>
</tr>
<tr>
<td>Name</td>
<td>My Theme</td>
<td>The scheme name visible to the end-user in the Predefined color scheme drop-down list in the DIP options. Do not enclose the name between <code>{}</code>.</td>
</tr>
<tr>
<td>GripColor</td>
<td></td>
<td>Color of the bar used to resize the number of available search interface tabs.</td>
</tr>
<tr>
<td>GripPointsColor</td>
<td></td>
<td>Color of the three dots in the bar used to resize the number of available search interface tabs.</td>
</tr>
<tr>
<td>MainColor</td>
<td></td>
<td>Main Sidebar color</td>
</tr>
</tbody>
</table>

To create a custom color scheme for the Outlook Sidebar in the Windows registry

1. Log in to a computer on which the Desktop Integration Package is installed.
2. Close Outlook.
3. Turn off the Desktop Integration Package by selecting the contextual menu of the Coveo Desktop Integration Package system icon ⚙, and then selecting Exit in the contextual menu.
4. Open the Windows Registry Editor (by pressing the Windows+r keys, and then typing regedit).
5. In the Registry Editor:
   a. Search or navigate to HKEY_CURRENT_USER > Software > Coveo > Search Bar > OutlookScheme.
   b. Right-click OutlookScheme, and then select New > Key.
   c. For the new folder, enter a name for your new color scheme. This name however is not the color scheme name that the end-user will see.
   d. Right-click the new folder, select New > String Value, and create each of the string values described in the following table.

<table>
<thead>
<tr>
<th>Name</th>
<th>Value (example)</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default</td>
<td>0</td>
<td>Set to 1 to make this scheme the default scheme.</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Important:</strong> Only one scheme must be the default theme otherwise the DIP will not start.</td>
</tr>
<tr>
<td>Name</td>
<td>My Theme</td>
<td>The scheme name visible to the end-user in the Predefined color scheme drop-down list in the DIP options. Do not enclose the name between <code>{}</code>.</td>
</tr>
<tr>
<td>GripColor</td>
<td></td>
<td>Color of the bar used to resize the number of available search interface tabs.</td>
</tr>
<tr>
<td>GripPointsColor</td>
<td></td>
<td>Color of the three dots in the bar used to resize the number of available search interface tabs.</td>
</tr>
<tr>
<td>MainColor</td>
<td></td>
<td>Main Sidebar color</td>
</tr>
</tbody>
</table>

To create a custom color scheme for the Outlook Sidebar in the Windows registry

1. Log in to a computer on which the Desktop Integration Package is installed.
2. Close Outlook.
3. Turn off the Desktop Integration Package by selecting the contextual menu of the Coveo Desktop Integration Package system icon ⚙, and then selecting Exit in the contextual menu.
4. Open the Windows Registry Editor (by pressing the Windows+r keys, and then typing regedit).
5. In the Registry Editor:
   a. Search or navigate to HKEY_CURRENT_USER > Software > Coveo > Search Bar > OutlookScheme.
   b. Right-click OutlookScheme, and then select New > Key.
   c. For the new folder, enter a name for your new color scheme. This name however is not the color scheme name that the end-user will see.
   d. Right-click the new folder, select New > String Value, and create each of the string values described in the following table.

<table>
<thead>
<tr>
<th>Name</th>
<th>Value (example)</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default</td>
<td>0</td>
<td>Set to 1 to make this scheme the default scheme.</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Important:</strong> Only one scheme must be the default theme otherwise the DIP will not start.</td>
</tr>
<tr>
<td>Name</td>
<td>My Theme</td>
<td>The scheme name visible to the end-user in the Predefined color scheme drop-down list in the DIP options. Do not enclose the name between <code>{}</code>.</td>
</tr>
<tr>
<td>GripColor</td>
<td></td>
<td>Color of the bar used to resize the number of available search interface tabs.</td>
</tr>
<tr>
<td>GripPointsColor</td>
<td></td>
<td>Color of the three dots in the bar used to resize the number of available search interface tabs.</td>
</tr>
<tr>
<td>MainColor</td>
<td></td>
<td>Main Sidebar color</td>
</tr>
<tr>
<td>Name</td>
<td>Value (example)</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------</td>
<td>-----------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>OutlookTheme</td>
<td>Leave this string empty. Used only for out-of-the-box schemes.</td>
<td></td>
</tr>
<tr>
<td>SearchButtonColor</td>
<td>Search button color</td>
<td></td>
</tr>
<tr>
<td>SearchButtonColorPressed</td>
<td>Search button color when pressed.</td>
<td></td>
</tr>
<tr>
<td>SidebarBorderColor</td>
<td>Color of the vertical bar used to resize the Sidebar.</td>
<td></td>
</tr>
<tr>
<td>TabColor</td>
<td>Tab text color when not selected neither hovered.</td>
<td></td>
</tr>
<tr>
<td>TabSelectedColor</td>
<td>Tab text color when selected.</td>
<td></td>
</tr>
<tr>
<td>TabHoveredColor</td>
<td>Tab text color when hovered.</td>
<td></td>
</tr>
<tr>
<td>TabSeparatorColor</td>
<td>Color of the tab separator</td>
<td></td>
</tr>
<tr>
<td>BrowserBackgroundColor</td>
<td>Background color of contact personal information zone</td>
<td></td>
</tr>
<tr>
<td>BrowserConversationSelectedColor</td>
<td>Highlight color for the selected email</td>
<td></td>
</tr>
<tr>
<td>BrowserStrokeColor</td>
<td>Color of lines separating various Sidebar sections</td>
<td></td>
</tr>
<tr>
<td>BrowserTabBackgroundColor</td>
<td>Tab background color</td>
<td></td>
</tr>
</tbody>
</table>

6. Restart the DIP by selecting the Windows Start button, typing Coveo Search Bar, and then pressing Enter.

7. Restart Outlook.

8. From the DIP options, select the newly created color scheme.

9. Validate that the scheme appears as expected.
4. Coveo Integration

This section contains procedures describing how to integrate Coveo search interfaces, or search boxes in other systems.

4.1 Integrating the Coveo .NET Search Interface in a Sitecore Website

Integrating the Coveo .NET search interface into Sitecore allows your end-users to search your Coveo index content directly from your Sitecore website using a feature-rich Coveo search interface.

**Note:** If not already done, index the content of your Sitecore site so you can include it in the scope of the search interface to integrate to Sitecore.

To integrate the Coveo search interface in a Sitecore website

1. Using an administrator account, log on to the Sitecore server.
2. If not already done, install or update the Coveo search interfaces on the Sitecore server.
3. Start the IIS Manager (on the Windows taskbar, select **Start > Administrative Tools > Internet Information Services (IIS) Manager**).
4. In **Internet Information Services (IIS) Manager**, create a virtual directory for your Sitecore web application:
   a. In the **Connections** panel, expand to the root of your Sitecore web application, right-click it and select **Add Virtual Directory**
b. In the Add Virtual Directory dialog box, enter Coveo in the Alias box and the [.NET_Front-End_Path]\Web\Coveo folder in the Physical path box.

5. Using a text editor:
   a. Open the Sitecore web.config file.

   **Note:** It is recommended to make a backup of the web.config file before editing it.

   b. In the configuration\configSections section, add the following code:
c. In the configuration \system.web\pages section, add the following code:

```xml
<sections>
  <sectionGroup name="coveoCnlWeb">
    <section name="customContent" type="System.Configuration.SingleTagSectionHandler, System, Version=1.0.3300.0, Culture=neutral, PublicKeyToken=b77a5c561934e089" />
  </sectionGroup>
  <sectionGroup name="coveoEnterpriseSearch">
    <section name="database" type="System.Configuration.SingleTagSectionHandler, System, Version=1.0.3300.0, Culture=neutral, PublicKeyToken=b77a5c561934e089" />
    <section name="analytics" type="System.Configuration.SingleTagSectionHandler, System, Version=1.0.3300.0, Culture=neutral, PublicKeyToken=b77a5c561934e089" />
    <section name="locations" type="System.Configuration.SingleTagSectionHandler, System, Version=1.0.3300.0, Culture=neutral, PublicKeyToken=b77a5c561934e089" />
    <section name="server" type="System.Configuration.SingleTagSectionHandler, System, Version=1.0.3300.0, Culture=neutral, PublicKeyToken=b77a5c561934e089" />
  </sectionGroup>
</sections>
```

```csharp
<controls>
  <add tagPrefix="cnla" namespace="Coveo.CNL.Web.Ajax" assembly="Coveo.CNL.Web, Version=12.0.0.0, Culture=neutral, PublicKeyToken=44110d16825221f2" />
  <add tagPrefix="cnlb" namespace="Coveo.CNL.Web.BetterControls" assembly="Coveo.CNL.Web, Version=12.0.0.0, Culture=neutral, PublicKeyToken=44110d16825221f2" />
  <add tagPrefix="cmlm" namespace="Coveo.CNL.Web.Misc" assembly="Coveo.CNL.Web, Version=12.0.0.0, Culture=neutral, PublicKeyToken=44110d16825221f2" />
  <add tagPrefix="cnlv" namespace="Coveo.CNL.Web.Validators" assembly="Coveo.CNL.Web, Version=12.0.0.0, Culture=neutral, PublicKeyToken=44110d16825221f2" />
  <add tagPrefix="cnlvs" namespace="Coveo.CNL.Web.Validators.ServerSide" assembly="Coveo.CNL.Web, Version=12.0.0.0, Culture=neutral, PublicKeyToken=44110d16825221f2" />
  <add tagPrefix="cnlw" namespace="Coveo.CNL.Web.Widgets" assembly="Coveo.CNL.Web, Version=12.0.0.0, Culture=neutral, PublicKeyToken=44110d16825221f2" />
  <add tagPrefix="ces" namespace="Coveo.CES.Web.Search.Controls" assembly="Coveo.CES.Web.Search, Version=12.0.0.0, Culture=neutral, PublicKeyToken=44110d16825221f2" />
  <add name="Coveo.CES.Web.Search" />
</controls>
```

d. In the configuration \system.web\compilation section, add the following code:

```xml
<assemblies>
  <add assembly="Coveo.CNL, Version=12.0.0.0, Culture=neutral, PublicKeyToken=44110d16825221f2" />
  <add assembly="Coveo.CNL.Web, Version=12.0.0.0, Culture=neutral, PublicKeyToken=44110d16825221f2" />
  <add assembly="Coveo.CES.Common, Version=12.0.0.0, Culture=neutral, PublicKeyToken=44110d16825221f2" />
  <add assembly="Coveo.CES.Web.Search, Version=12.0.0.0, Culture=neutral, PublicKeyToken=44110d16825221f2" />
</assemblies>
```

e. In the configuration section, add the following code:

```xml
<vector>
  <add name="Coveo.CNLWeb" />
  <add name="Coveo.CES.WebSearch" />
</vector>
```
f. Save the file.

6. Integrate the search interface in a Sitecore layout or sublayout:

- Add the following code at the appropriate location in the Sitecore .aspx layout or sublayout file in which you want to integrate the Coveo search interface control.

```csharp
<%@ Register TagPrefix="ces" Namespace="Coveo.CES.Web.Search.Controls" Assembly="Coveo.CES.Web.Search, Version=12.0.0.0, Culture=neutral, PublicKeyToken=44110d16825221f2" %>
<%@ Assembly Name="Coveo.CNL, Version=12.0.0.0, Culture=neutral, PublicKeyToken=44110d16825221f2" %>
<%@ Assembly Name="Coveo.CNL.Web, Version=12.0.0.0, Culture=neutral, PublicKeyToken=44110d16825221f2" %>
<asp:Panel ID="pnResultsPanel" runat="server">
  <ces:SearchHub id="c" runat="server" />
</asp:Panel>

OR

a. When you chose to index Sitecore security using a security provider, you must rather add the following code that includes a script to allow the search interface to display the search results corresponding to the currently logged on user.

Using the Sitecore API, the _OverrideUser script retrieves the currently logged on user and passes this user to the Coveo search Interface.

**Note:** CES security elements are case sensitive. The Sitecore connector always indexes security elements in lower-case. Ensure to provide a lower-case username for the security to be resolved correctly.

```csharp
<%@ Control Language="C#" AutoEventWireup="true" Inherits="layouts_PFCEnergy_CoveoSearchResults" Codebehind="CoveoSearchResults.ascx.cs" %>
<%@ Register TagPrefix="ces" Namespace="Coveo.CES.Web.Search.Controls" Assembly="Coveo.CES.Web.Search, Version=12.0.0.0, Culture=neutral, PublicKeyToken=44110d16825221f2" %>
<%@ Assembly Name="Coveo.CNL, Version=12.0.0.0, Culture=neutral, PublicKeyToken=44110d16825221f2" %>
<%@ Assembly Name="Coveo.CNL.Web, Version=12.0.0.0, Culture=neutral, PublicKeyToken=44110d16825221f2" %>
<script runat="server">
  void _OverrideUser(object p_Sender, Coveo.CES.Web.Search.Controls.OverrideUserEventArgs p_Args)
  {
    // The name of the security provider defined under the Admin Tool
    string securityProviderName = "Sitecore Security Provider";
    // Get the username from SitecoreAPI
    string userName = Sitecore.Context.GetUserName().ToLower();
    // Add to the collection of identities
    Coveo.CES.Web.Search.Providers.IUserIdentity user = factory.CreateSecurityProviderUser(userName, securityProviderName, false, null);
    p_Args.AdditionalIdentities.Add(user);
  }
</script>
```
Note: OnOverrideUser event is not available for all Coveo search controls such as QuickSearch and SearchBox controls.

The search interface can target an explicit index source as shown in the following script.

```csharp
<script runat="server">
override void OnInit(EventArgs p_Args)
{
    SearchBinding.MainSearchObject.SetupSearchBuilder += this.Search_SetupSearchBuilder;
    base.OnInit(p_Args);
}
void Search_SetupSearchBuilder(object p_Sender, SetupSearchBuilderEventArgs p_Args)
{
    p_Args.Builder.AddConstantExpression("@Source=MySourceName");
}
</script>
```

7. Using a browser, access the modified page to view the search hub.

The Front-End Server Configuration first time setup page appears to allow you to complete the Coveo Front-End installation.

Tip: If you notice that some of Coveo images or JavaScript are missing because they do not load in the search interface, you can fix this problem with a simple edit of the Sitecore web.config file (not the Coveo web.config file). In the file, locate the `<setting name="IgnoreUrlPrefixes" ...>` tag and add the `|/Coveo/` string to the value attribute.

Example:

```xml
<setting name="IgnoreUrlPrefixes"
value="/sitecore/default.aspx|/trace.axd|/webresource.axd|/Coveo/"/>
```

What's Next?

Consider also integrating the Coveo search in the Sitecore Content Editor (see "Integrating the Coveo .NET Search in the Sitecore Content Editor" on page 163).

4.2 Integrating the Coveo .NET Search in the Sitecore Content Editor

You can integrate the Coveo .NET search interfaces in your Sitecore website to provide a better search experience to your website users (see "Integrating the Coveo .NET Search Interface in a Sitecore Website" on page 158).

You can also integrate the Coveo search in the Sitecore Content Editor so that people contributing to the site content can also take advantage of the Coveo search features and more easily find information in the whole content, not just published content.

Note: The integration described in this topic works with Coveo .NET Front-End 12.0.61+.
Tip: Typically, a Sitecore site is managed with a Master database containing the whole content and a Web database containing only the published content. You can create separate sources for these two databases, and then assign the Web source to the scope of the search interface integrated in the website, and the Master source to the scope of the search interface integrated in the Content Editor. This way, all of the unpublished content is searchable from the Sitecore Desktop.

To integrate the Coveo search in the Sitecore Content Editor

1. If not already done, install the Coveo Front-End components on your Sitecore server.
2. Install the Coveo Content Search for Sitecore:
   a. Log in to the Sitecore Desktop user interface using an administrative account.
c. In the **Installation Wizard** dialog box:

   i. In the **Welcome to the Install Package Wizard** screen, click **Next**.

   ii. In the **Select Package** screen:

      i. Click **Upload**, and then browse the Coveo Master server to select the Coveo Content Search package distributed with CES:

      ![Image of Coveo Installation Wizard]

      

      [CES_Install_Path]\Bin\Sitecore6.0CoveoContentSearch2.zip

      **Note:** Use the `Sitecore6.0CoveoContentSearch.zip` package only when you use the Sitecore legacy connector.

      ii. Click **Next**.

      iii. In the **Ready to Install** screen, click **Install**.

      **Note:** If an Access Denied error is displayed for the `bin_install` folder while installing the package, verify the security permissions for ASP.NET in the bin folder of Sitecore or install the files manually.

d. Select the **Restart the Sitecore client** option, and then click **Finish**.

3. Using an administrator account, connect to your Sitecore server.

4. Create the Coveo virtual directory:

   a. Open IIS.

   b. In IIS, locate and right-click the website that corresponds to your Sitecore instance, and then select **Add virtual directory**.

   c. In the **Create Virtual Directory** dialog box:

      i. In the **Alias** box, enter Coveo.

      ii. In the **Physical path** box, enter `.NET_Front-End_Path]\Web\Coveo`, typically `C:\Program Files\Coveo .NET Front-End 12\Web\Coveo`.

   d. Close IIS.
5. Using a text editor, edit the Sitecore web.config file:

Example: For an instance named Sitecore, the file is located in the
C:\inetpub\wwwroot\Sitecore\WebSite folder.

a. Copy the following code and paste it just before the </configSections> tag.

```
<sectionGroup name="coveoCnlWeb">
    <section name="customContent" type="System.Configuration.SingleTagSectionHandler, System, Version=1.0.3300.0, Culture=neutral, PublicKeyToken=b77a5c561934e089" />
</sectionGroup>
<sectionGroup name="coveoEnterpriseSearch">
    <section name="database" type="System.Configuration.SingleTagSectionHandler, System, Version=1.0.3300.0, Culture=neutral, PublicKeyToken=b77a5c561934e089" />
    <section name="analytics" type="System.Configuration.SingleTagSectionHandler, System, Version=1.0.3300.0, Culture=neutral, PublicKeyToken=b77a5c561934e089" />
    <section name="locations" type="System.Configuration.SingleTagSectionHandler, System, Version=1.0.3300.0, Culture=neutral, PublicKeyToken=b77a5c561934e089" />
    <section name="server" type="System.Configuration.SingleTagSectionHandler, System, Version=1.0.3300.0, Culture=neutral, PublicKeyToken=b77a5c561934e089" />
</sectionGroup>
```

b. Copy the following code and paste it just before the </controls> tag, a child of the <pages> tag.

```
<add tagPrefix="cnla" namespace="Coveo.CNL.Web.Ajax" assembly="Coveo.CNL.Web, Version=12.0.0.0, Culture=neutral, PublicKeyToken=44110d16825221f2" />
<add tagPrefix="cnlb" namespace="Coveo.CNL.Web.BetterControls" assembly="Coveo.CNL.Web, Version=12.0.0.0, Culture=neutral, PublicKeyToken=44110d16825221f2" />
<add tagPrefix="cnlm" namespace="Coveo.CNL.Web.Misc" assembly="Coveo.CNL.Web, Version=12.0.0.0, Culture=neutral, PublicKeyToken=44110d16825221f2" />
<add tagPrefix="cnlv" namespace="Coveo.CNL.Web.Validators" assembly="Coveo.CNL.Web, Version=12.0.0.0, Culture=neutral, PublicKeyToken=44110d16825221f2" />
```

c. Copy the following code and paste it just before the </namespace> tag, a child of the <namespaces> tag.

```
<add namespace="Coveo.CES.Web.Search.Controls" />
<add namespace="Coveo.CNL.Web" />
```

d. Copy the following code and paste it just before the </assemblies> tag, a child of the <compilation> tag.

```
<add assembly="Coveo.CNL, Version=12.0.0.0, Culture=neutral, PublicKeyToken=44110d16825221f2" />
<add assembly="Coveo.CES.Common, Version=12.0.0.0, Culture=neutral, PublicKeyToken=44110d16825221f2" />
<add assembly="Coveo.CNL.Web, Version=12.0.0.0, Culture=neutral, PublicKeyToken=44110d16825221f2" />
<add assembly="Coveo.CES.Web.Search, Version=12.0.0.0, Culture=neutral, PublicKeyToken=44110d16825221f2" />
```

e. Copy the following code and paste it at the end of the file, just before the </configuration> tag.
f. Save the file.

6. When CES and Sitecore are not installed on the same server, copy the index certificate file from the Coveo Master server to the Sitecore server:
   
a. Using an administrator account, connect to the Coveo Master server.
   
b. Copy the index certificate file \[Index\_Path\]\Config\Certificates\cert-iis.p12, typically C:\CES7\Config\Certificates\cert-iis.p12.
   
c. Paste the certificate file on the Sitecore server into the Sitecore instance website.
   
   Example: For an instance named Sitecore, the default path is C:\inetpub\wwwroot\Sitecore\Website. You can also rename the certificate file such as ces-certificate.p12.

7. Configure the connection to the CES index. Using a text editor:
   
a. Open the Sitecore instance web.config file.
   
b. Under the <coveoEnterpriseSearch> tag, edit the <server> tag to include the following attributes:
      
      - hostname="MyCoveoMasterServerHostName" where you replace MyCoveoMasterServerHostName with the name of your Coveo Master server or localhost when CES and Sitecore are on the same machine.
      
      - sslCertificatePath="C:\inetpub\wwwroot\Sitecore\Website\ces-certificate.p12", ensuring that the path points to your certificate file.
      
      - port="52800", the default CES port number.

   Example: When CES and Sitecore are on the same server.

   ```xml
   <server hostname="localhost" port="52800" servicesHostname="localhost" servicesPort="52810" instance="default" mirrorName="default" sslCertificatePath="C:\Program Files\Coveo .NET Front-End 12\Web\ces-certificate.p12"/>
   ```

8. Configure the Sitecore source used by Coveo search:
   
a. Using a text editor, open the CoveoSearch.aspx file.
   
   Example: For a Sitecore instance named Sitecore, the file is typically located in the C:\inetpub\wwwroot\Sitecore\Website\sitecore\shell\Applications\Coveo\ folder.
   
b. Locate the following code:
/* UNCOMMENT THIS SECTION BEFORE FIRST USE
p_Args.Builder.AddConstantExpression("@Source=MySourceName");
*/

and replace it with:

```javascript
p_Args.Builder.AddConstantExpression("@Source="YOUR SITECORE SOURCE NAME HERE"";
```

where you replace YOUR SITECORE SOURCE NAME HERE by the name of the source you created to contain the whole Sitecore content, typically indexing the master database.

c. Save and close the file.

4.3 Coveo JavaScript Search Framework

The Coveo JavaScript Search Framework provides a set of search interface components that you can use as building blocks to create feature-rich search interfaces. The framework also comes with a set of out-of-the-box search interfaces that you can easily customize and deploy.

The JavaScript Search Framework is bundled with other Coveo products (Coveo for Salesforce, Coveo for Sitecore, "Coveo REST Search API 8.0" on page 70) but can also be integrated in a web site (see "Coveo Platform On-Premises Products" on page 245).

Integrators and administrators can easily customize Coveo for Salesforce search interfaces using the Interface Editor (see JavaScript Search Interface Editor or JavaScript Search Legacy Interface Editor Overview) while developers can directly add, remove, or customize search interface components by modifying the page HTML markup with appropriate framework attributes and CSS classes (see Getting Started with the JavaScript Search Framework V1).
4.4 Integrating a .NET Search Hub in ASP

The Coveo .NET Front-End search hub is referenced in the default document defined in IIS for your Coveo search website.

Example: When you install CES in the default installation folder, the installer creates the default Coveo Enterprise Search 7 website, the default document defined in IIS for the website is the C:\Program Files\Coveo .NET Front-End 12\Web\Coveo\default.aspx file and the default search hub is referenced in this file by the <ces:SearchHub id="h" runat="server"/> code line.

When you create a new search hub, you can use it by referencing it in the default document defined in IIS for your website or in other custom ASP pages that you may want to create and use in other contexts.

To integrate a Coveo search hub to an ASP.NET page

1. Using an administrator account, connect to the server for the website in which you want to integrate the Coveo search hub.

2. Using a text editor:
a. Open the .aspx file for the ASP.NET page in which you want to integrate the Coveo search hub.

b. Add or ensure that the following declaration appears after the @page directive.

```csharp
<%@ Register TagPrefix="ces" Namespace="Coveo.CES.Web.Search.Controls" Assembly="Coveo.CES.Web.Search, Version=12.0.0.0, Culture=neutral, PublicKeyToken=44110d16825221f2" %>
```

c. Locate the place where the search hub is to be inserted (such as after the custom page headers) and add or edit the following control:

```csharp
<ces:SearchHub Name="MyHubName" runat="server" />
```

where you replace MyHubName by the name of your search hub.

**Note:** The ces:SearchHub control must be inserted in the ASPX page in the existing `<form>` node, or in a unique new one if none exists.

d. Save the modifications.

3. In IIS, for the site containing the page in which you integrate the search hub, create a virtual folder named Coveo that points to the `\[.NET_Front-End_Path]\Web\Coveo` folder (see the Microsoft document Create a Virtual Directory (IIS 7)).

4. Using a text editor:

a. Open the web.config file of the site in which you are integrating the Coveo search hub.

b. Add the following definitions to the `Configuration > ConfigSections` section.

```csharp
<sectionGroup name="coveoCnlWeb">
  <section name="customContent" type="System.Configuration.SingleTagSectionHandler, System, Version=1.0.3300.0, Culture=neutral, PublicKeyToken=b77a5c561934e089" />
</sectionGroup>

<sectionGroup name="coveoEnterpriseSearch">
  <section name="database" type="System.Configuration.SingleTagSectionHandler, System, Version=1.0.3300.0, Culture=neutral, PublicKeyToken=b77a5c561934e089" />
  <section name="analytics" type="System.Configuration.SingleTagSectionHandler, System, Version=1.0.3300.0, Culture=neutral, PublicKeyToken=b77a5c561934e089" />
  <section name="locations" type="System.Configuration.SingleTagSectionHandler, System, Version=1.0.3300.0, Culture=neutral, PublicKeyToken=b77a5c561934e089" />
  <section name="server" type="System.Configuration.SingleTagSectionHandler, System, Version=1.0.3300.0, Culture=neutral, PublicKeyToken=b77a5c561934e089" />
</sectionGroup>
```

c. In the `configuration>ConfigSections` section, add the following code:

```csharp
<sectionGroup name="coveoCnlWeb">
  <section name="customContent" type="System.Configuration.SingleTagSectionHandler, System, Version=1.0.3300.0, Culture=neutral, PublicKeyToken=b77a5c561934e089" />
</sectionGroup>

<sectionGroup name="coveoEnterpriseSearch">
  <section name="database" type="System.Configuration.SingleTagSectionHandler, System, Version=1.0.3300.0, Culture=neutral, PublicKeyToken=b77a5c561934e089" />
  <section name="analytics" type="System.Configuration.SingleTagSectionHandler, System, Version=1.0.3300.0, Culture=neutral, PublicKeyToken=b77a5c561934e089" />
  <section name="locations" type="System.Configuration.SingleTagSectionHandler, System, Version=1.0.3300.0, Culture=neutral, PublicKeyToken=b77a5c561934e089" />
  <section name="server" type="System.Configuration.SingleTagSectionHandler, System, Version=1.0.3300.0, Culture=neutral, PublicKeyToken=b77a5c561934e089" />
</sectionGroup>
```
d. In the configuration\system.web\pages section, add the following code:

```xml
<controls>
  <add tagPrefix="cnla" namespace="Coveo.CNL.Web.Ajax" assembly="Coveo.CNL.Web, Version=12.0.0.0, Culture=neutral, PublicKeyToken=44110d16825221f2" />
  <add tagPrefix="cnlb" namespace="Coveo.CNL.Web.BetterControls" assembly="Coveo.CNL.Web, Version=12.0.0.0, Culture=neutral, PublicKeyToken=44110d16825221f2" />
  <add tagPrefix="cnlm" namespace="Coveo.CNL.Web.Misc" assembly="Coveo.CNL.Web, Version=12.0.0.0, Culture=neutral, PublicKeyToken=44110d16825221f2" />
  <add tagPrefix="cnlv" namespace="Coveo.CNL.Web.Validators" assembly="Coveo.CNL.Web, Version=12.0.0.0, Culture=neutral, PublicKeyToken=44110d16825221f2" />
  <add tagPrefix="cnlvs" namespace="Coveo.CNL.Web.Validators.ServerSide" assembly="Coveo.CNL.Web, Version=12.0.0.0, Culture=neutral, PublicKeyToken=44110d16825221f2" />
  <add tagPrefix="cnlw" namespace="Coveo.CNL.Web.Widgets" assembly="Coveo.CNL.Web, Version=12.0.0.0, Culture=neutral, PublicKeyToken=44110d16825221f2" />
  <add tagPrefix="ces" namespace="Coveo.CES.Web.Search.Controls" assembly="Coveo.CES.Web.Search, Version=12.0.0.0, Culture=neutral, PublicKeyToken=44110d16825221f2" />
</controls>

<namespaces>
  <add namespace="Coveo.CES.Web.Search" />
  <add namespace="Coveo.CES.Web.Search.Controls" />
  <add namespace="Coveo.CNL.Web" />
</namespaces>
```

e. In the configuration\system.web\compilation section, add the following code:

```xml
<assemblies>
  <add assembly="Coveo.CNL, Version=12.0.0.0, Culture=neutral, PublicKeyToken=44110d16825221f2" />
  <add assembly="Coveo.CNL.Web, Version=12.0.0.0, Culture=neutral, PublicKeyToken=44110d16825221f2" />
  <add assembly="Coveo.CES.Common, Version=12.0.0.0, Culture=neutral, PublicKeyToken=44110d16825221f2" />
  <add assembly="Coveo.CES.Web.Search, Version=12.0.0.0, Culture=neutral, PublicKeyToken=44110d16825221f2" />
</assemblies>
```

f. In the configuration section, add the following code:

```xml
<coveoCnlWeb>
  <customContent url="/Coveo/" anonymousUrl="/Coveo/Anonymous/" />
</coveoCnlWeb>
<coveoEnterpriseSearch>
  <server hostname="localhost" port="52800" servicesHostname="localhost" servicesPort="52810" instance="default" mirrorName="default" sslCertificatePath="C:\Program Files\Coveo .NET Front-End 12\Web\certificate.p12" />
  <database enabled="false" connectionString="mongodb://localhost/databaseName" />
  <analytics enabled="false" connectionString="Data Source=yourServerName;Initial Catalog=CoveoAnalytics;Integrated Security=SSPI;" />
</coveoEnterpriseSearch>
```

g. Save the file.

5. Using a browser, access the modified page to attempt to view the search hub.

The Front-End Server Configuration first time setup page appears to allow you to complete the installation (see "Coveo .NET Front-End First Time Setup" on page 47).
### 4.5 Enabling the Scope Selector in Microsoft SharePoint

In Microsoft SharePoint, the scope selector is a control that you can add next to the Coveo search box to allow users to select the scope in which the search should be performed. Scopes are defined by the administrator.

![Image of scope selector](image)

1. Scope selector
2. Coveo search box integrated in Microsoft SharePoint

As a Coveo administrator, you can enable the scope selector in Microsoft SharePoint by editing the `searchBox.ascx` file in the skin used by your SharePoint interface.

**Note:** In the case of a SharePoint farm, you must perform the following procedure for each SharePoint server.

To enable the scope selector in Microsoft SharePoint:

1. Using an administrator account, connect to the SharePoint server on which Coveo is installed.

   **Important:** It is not recommended to customize the default skins provided by Coveo. Default skins are overwritten when upgrading CES. The best practice is to create a renamed copy of the default skin, and then modify and use the new skin.

2. Unless you are already using a custom skin, in the `\[.NET_Front-End_Path]\Web\Coveo\Skins\` folder:
   
   a. Make a copy of the `SharePoint` folder.
   
   b. Rename the folder copy to the name of your choice.
Example: SharePointScopeSelector

3. Using a text editor:
   a. Open the searchBox.ascx file from your new skin folder.
   b. Add the following lines of code:

   ```html
   <td style="padding-right: 2px">
     <select id="DDLScope" runat="server"/>
   </td>
   ```

   as shown in the following excerpt (after line 12):

   ```html
   <table cellspacing="0" cellpadding="0">
     <tr>
       <td>
         <input type="text" id="TXTQuery" style="font-size: 9pt" runat="server"/>
       </td>
       <td style="padding-left: 2px">
         <% ((BetterImage) BTNSearch).ImageUrl = SearchBox.SearchImage.Resolve(); %>
         <% ((BetterImage) BTNSearch).HoveredImageUrl = SearchBox.SearchHoveredImage.Resolve(); %>
         <% ((BetterImage) BTNSearch).ToolTip = SearchStrings.Search; %>
         <% ((BetterImage) BTNSearch).Style["cursor"] = "pointer"; %>
         <cnlb:BetterImage id="BTNSearch" runat="server"/>
       </td>
       <td style="padding-right: 2px">
         <select id="DDLScope" runat="server"/>
       </td>
     </tr>
   </table>
   ```

   c. Save the file.

4. Reset IIS on the server to make the changes effective.

5. Unless you modified an existing custom skin, you must now configure the SharePoint search interface to use the new skin that you created:
   a. Using a Coveo administrator account, access a SharePoint page where the Coveo search box appears, and then launch any query to open the search interface.
   b. In the upper-right corner of the .NET search interface, in the Do More menu, select Edit this Interface.

   **Note:** The Edit this Interface command of the Do More menu only appears for a Coveo administrator.

   The Interface Editor opens with the SharePoint interface as the current interface.

   c. Under Basic Configuration, in the Skin drop-down list, select the new skin that you created.

   **Note:** The new skin will appear only after performing the IIS reset.

   d. Click Apply.

6. Validate that the scope selector is available to users: 
a. Clear the cache of your browser and then close the browser.

b. Restart the browser, open a SharePoint page where the Coveo search box appears to verify that the scope selector appears next to the search box.

4.6 Modifying the Language of the .NET Search Interface

Coveo .NET Front-End search interface templates are available in English (default.aspx), French (default-fr.aspx), Spanish (default-es.aspx), and German (default-de.aspx). You can use a .NET search interface in a different language by inserting the appropriate template name in the address.


To add a link pointing to a .NET search interface in another language

1. In a text editor, open the appropriate template (ex.: default.aspx).
2. After the <body> tag, enter a link in the form:

   <a href="default-fr.aspx">Français</a>

   where default-fr.aspx can be replaced by the appropriate template and Français by the appropriate language.
3. Save the file.

4.7 Integrating a Coveo .NET Search Interface in a non ASP.NET Site

It is possible to integrate a Coveo .NET search interface into an HTML page hosted on a non ASP.NET Web server using a JavaScript/AJAX. This technique involves configuring a reverse proxy to route the search requests from the client computer to the Coveo server and the search results back to the client computer. This process is transparent to the end-user. Contact the Coveo Professional Services for assistance.

You must set up the following elements to use the bootstrapper:

- An iframe that handles the navigation history.
- A script tag that loads the Coveo JavaScript Library.
- A div placeholder tag in which the Coveo controls are inserted.
- A script tag that calls the Coveo library to insert content into the placeholder.

To bootstrap a Coveo .NET search interface in a non .NET HTML page

1. Using an administrator account, connect to the Coveo Master server.
2. In Internet Information Services (IIS) Manager:
a. Add a new Website named Bootstrap.
b. Under the Bootstrap Website, create a new Virtual Directory named CES7.
c. Create an Application named CES7
d. Set the local path to [CES_Install_Path]\Web.

3. Using a text editor:
   a. Create a default.htm file at the root of the Bootstrap Website.
   b. Paste the following code in the file.

   ```html
   <html>
   <body>
   <iframe id="_historyFrame" src="empty.htm" style="display:none"></iframe>
   <script type="text/javascript" src="/CES6/Coveo/CustomContent.aspx?k=embedding"></script>
   <div id="here">Loading...</div>
   <script>
   document.getElementById('here'),true);
   </script>
   </body>
   </html>
   ```
   c. Save the file.


4.8 Searching and Retrieving Results Using XML Search

The Coveo .NET Front-End can return search results in an XML format. Using XML search is useful to easily integrate Coveo search results in a third-party application or a website without making calls to the Coveo API. This is done using the basic HTTP request/response communications to integrate search results in a web access point.

**Example:** To add search results to a website using XML search:

1. Add an XML Search page to your site.
2. Perform a search using the Coveo XML Search page.
3. Parse the XML to display results.

You can obtain XML search results using the XMLsearch.aspx in the search URL of the form:

http://[CoveoServer]/XMLSearch.aspx?[Query]
Example: Searching for united oil financial statements year ended 2003 from the intranet search interface on a Coveo server returns 4 results. Using the following URL from this Coveo server:

https://localhost/XMLsearch.aspx?BasicQuery=united oil financial statements year ended 2003 @sysspversion
	no results, but in the following XML format:

```
<QueryResults xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns:xsd="http://www.w3.org/2001/XMLSchema">
  <BasicQuery>true</BasicQuery>
  <BasicQuery>united oil financial statements year ended 2003 @sysspversion</BasicQuery>
  <AdvancedQuery/>
  <ExpandedQuery/>
  <TotalCount>4</TotalCount>
  <Time>0.047</Time>
  <Filtered>false</Filtered>
  <Optimized>false</Optimized>
  <TotalCount>4</TotalCount>
  <Time>0.047</Time>
  <Filtered>false</Filtered>
  <Optimized>false</Optimized>
  <Results>
    <QueryResult>
      <UniqueId>172622!-</UniqueId>
      <Title>Financial funding United Oil Draft</Title>
      <Uri>https://sp2010.demo.coveo.com/Finance/Shared Documents/Funding Reports/Financial funding United oil Sharepoint.docx</Uri>
      <PrintableUri>https://sp2010.demo.coveo.com/Finance/Shared Documents/Funding Reports/Financial funding United oil Sharepoint.docx</PrintableUri>
      <TargetUri>https://sp2010.demo.coveo.com/Finance/Shared Documents/Funding Reports/Financial funding United oil Sharepoint.docx</TargetUri>
      <Score>2710</Score>
      <PercentageScore>52.327528381347656</PercentageScore>
      <Size>293386</Size>
      <IsAttachment>false</IsAttachment>
      <ContainsAttachment>true</ContainsAttachment>
      <ModifiedDate>2010-09-21T18:39:25</ModifiedDate>
      <IndexedDate>2011-03-01T16:36</IndexedDate>
      <IsTopResult>false</IsTopResult>
      <Rating>3</Rating>
      <IsUserRating>false</IsUserRating>
      <LastView>0001-01-01T00:00:00</LastView>
      <NumberOfViews>0</NumberOfViews>
    </QueryResult>
    <QueryResult>...</QueryResult>
    <QueryResult>...</QueryResult>
    <QueryResult>...</QueryResult>
  </Results>
  <ExceptionCode>1</ExceptionCode>
  <ExceptionContext/>
</QueryResults>
```

Note: The XML search results output does not feature all the controls of the default search interface. For example, the facets are not included.

4.8.1 Available Parameters

In the query, you can use the parameters described in the following table.
<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
<th>Possible Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>AdvancedQuery</td>
<td>String</td>
<td>Advanced query expression.</td>
<td>(according to search syntax)</td>
</tr>
<tr>
<td>AllRemoteServers</td>
<td>Boolean</td>
<td>Set to true to include all remote servers in the query.</td>
<td>[true, false]</td>
</tr>
<tr>
<td>BasicQuery</td>
<td>String</td>
<td>Basic query expression.</td>
<td>(according to search syntax)</td>
</tr>
<tr>
<td>CollectionIds</td>
<td>Comma separated string</td>
<td>IDs of the collections in which the query should be performed.</td>
<td>If no collections are specified, then they are all selected.</td>
</tr>
<tr>
<td>CollectionNames</td>
<td>Comma separated string</td>
<td>Names of the collections in which the query should be performed.</td>
<td>Available collections. If collections specified do not exist, they are dismissed.</td>
</tr>
<tr>
<td>DefaultTimeOut</td>
<td>Integer</td>
<td>The timeout delay to use when querying remote servers (in milliseconds). Used only when AllRemoteServers is true.</td>
<td>[0...]</td>
</tr>
<tr>
<td>DoNotLog</td>
<td>Boolean</td>
<td>Set to true to disable query logging.</td>
<td>[true, false]</td>
</tr>
<tr>
<td>ExcerptLength</td>
<td>Integer</td>
<td>Length of the excerpt to retrieve for each result (in characters). Set this property to a non-zero value to retrieve an excerpt.</td>
<td>[0...]</td>
</tr>
<tr>
<td>ExpandQuery</td>
<td>Boolean</td>
<td>Set to true to enable query expansion using the thesaurus.</td>
<td>[true, false]</td>
</tr>
<tr>
<td>FilterByField</td>
<td>String</td>
<td>The custom field to use for filtering custom duplicates.</td>
<td>Any available field, prefixed by @</td>
</tr>
<tr>
<td>FilterDuplicates</td>
<td>Boolean</td>
<td>Set to true to enable duplicate document filtering.</td>
<td>[true, false]</td>
</tr>
<tr>
<td>FirstResult</td>
<td>Integer</td>
<td>0-based index of the first result to retrieve.</td>
<td>[0...49999]</td>
</tr>
<tr>
<td>ImpersonatorChain</td>
<td>Comma separated string</td>
<td>Authentication information (chain of users to impersonate) for the execution of the query.</td>
<td></td>
</tr>
<tr>
<td>NeedCachedDocumentUris</td>
<td>Boolean</td>
<td>Set to true to retrieve the URIs that serve cached versions of the results.</td>
<td>[true, false]</td>
</tr>
<tr>
<td>Name</td>
<td>Type</td>
<td>Description</td>
<td>Possible Values</td>
</tr>
<tr>
<td>-------------------</td>
<td>------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>---------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>NeedConcepts</td>
<td>Boolean</td>
<td>Set to <code>true</code> to retrieve the concepts for each result.</td>
<td><code>[true, false]</code></td>
</tr>
<tr>
<td>NeededFields</td>
<td>Comma separated string</td>
<td>List of fields whose value should be retrieved.</td>
<td>Any available field, prefixed by <code>@</code></td>
</tr>
<tr>
<td>NeedHighlights</td>
<td>Boolean</td>
<td>Set to <code>true</code> to retrieve the highlights for the title, excerpt, etc.</td>
<td><code>[true, false]</code></td>
</tr>
<tr>
<td>NeedParsedQuery</td>
<td>Boolean</td>
<td>Set to <code>true</code> to retrieve the parsed query information. When performing a query, the parsed information is available in <code>QueryResults.ParsedQuery</code>.</td>
<td><code>[true, false]</code></td>
</tr>
<tr>
<td>NeedQueryCorrections</td>
<td>Boolean</td>
<td>Set to <code>true</code> to retrieve the potential query corrections.</td>
<td><code>[true, false]</code></td>
</tr>
<tr>
<td>NumberOfResults</td>
<td>Integer</td>
<td>Maximum number of results to retrieve.</td>
<td><code>[1…50000]</code></td>
</tr>
<tr>
<td>Optimize</td>
<td>Boolean</td>
<td>Set to <code>true</code> to enable exact string query optimizations.</td>
<td><code>[true, false]</code></td>
</tr>
<tr>
<td>PreferredLanguage</td>
<td>String</td>
<td>Optional name of the preferred language for results.</td>
<td><code>[english,french]</code></td>
</tr>
<tr>
<td>SavedQueryOrFilter</td>
<td>String</td>
<td>The serialized saved query or filter to include in the search.</td>
<td></td>
</tr>
<tr>
<td>SortByField</td>
<td>String</td>
<td>Optional name of the field to use for sorting results.</td>
<td>(according to fields configured as sortable) Used only if <code>SortCriteria</code> is in <code>[FieldAscending, FieldDescending]</code></td>
</tr>
<tr>
<td>SortCriteria</td>
<td>String</td>
<td>Sort criteria to use for sorting results. Note: in versions prior to 14.13.1808 this parameter was named <code>SortBy</code>.</td>
<td><code>[Relevancy, ModifiedDateAscending, ModifiedDateDescending, FieldAscending, FieldDescending]</code></td>
</tr>
<tr>
<td>SummaryLength</td>
<td>Integer</td>
<td>Length of the summary to retrieve for each result (in words). Set this property to a non-zero value to retrieve a summary.</td>
<td><code>[0…]</code></td>
</tr>
<tr>
<td>Name</td>
<td>Type</td>
<td>Description</td>
<td>Possible Values</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>----------</td>
<td>-----------------------------------------------------------------------------</td>
<td>------------------------------</td>
</tr>
<tr>
<td>TimeZoneOffset</td>
<td>Integer</td>
<td>End user's offset from local time to UTC, in minutes.</td>
<td>[-720...720]</td>
</tr>
<tr>
<td>UseCollaborativeRanking</td>
<td>Boolean</td>
<td>Set to true to enable collaborative ranking for this query.</td>
<td>[true, false]</td>
</tr>
<tr>
<td>UseWildcards</td>
<td>Boolean</td>
<td>Set to true to enable wildcards for this query.</td>
<td>[true, false]</td>
</tr>
</tbody>
</table>

**Example:** A more complex query combining several parameters:

http://localhost/XMLSearch.aspx?BasicQuery=@uri&collectionnames=portal,test&NumberOfResults=4&SortBy=ModifiedDateDescending
&ExcerptLength=200&SummaryLength=60&NeedConcepts=true

4.8.2 Output XML Schema

```xml
<QueryResults xmlns:xsd="http://www.w3.org/2001/XMLSchema"
               xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
  <Executed></Executed>
  <BasicQuery></BasicQuery>
  <AdvancedQuery></AdvancedQuery>
  <ExpandedQuery></ExpandedQuery>
  <TotalCount></TotalCount>
  <Time></Time>
  <Filtered></Filtered>
  <Optimized></Optimized>
  <QueryCorrections>
    <QueryCorrection>
      <CorrectedQuery></CorrectedQuery>
      <WordCorrections>
        <WordCorrection>
          <Position></Position>
          <OriginalWord></OriginalWord>
          <CorrectedWord></CorrectedWord>
        </WordCorrection>
      </WordCorrections>
    </QueryCorrection>
  </QueryCorrections>
  <Results>
    <QueryResult>
      <UniqueId></UniqueId>
      <Title></Title>
      <TitleHighlights>
        <Highlight>
          <Position></Position>
          <Length></Length>
        </Highlight>
      </TitleHighlights>
      <Uri></Uri>
      <PrintableUri></PrintableUri>
      <PrintableUriHighlights>
        <Highlight>
          <Position></Position>
          <Length></Length>
        </Highlight>
      </PrintableUriHighlights>
      <Score></Score>
      <Size></Size>
    </QueryResult>
  </Results>
</QueryResults>
```
<IsAttachment></IsAttachment>  
<ContainsAttachment></ContainsAttachment>  
<ModifiedDate></ModifiedDate>  
<IndexedDate></IndexedDate>  
<Field>  
<ResultField>  
<Name></Name>  
<Value xsi:type=""></Value>  
</ResultField>  
</Field>  
<IsTopResult></IsTopResult>  
<Rating></Rating>  
<IsUserRating></IsUserRating>  
>LastView></LastView>  
<NumberofViews></NumberofViews>  
<Excerpt></Excerpt>  
<ExcerptHighlights>  
<Highlight>  
<Position></Position>  
<Length></Length>  
</Highlight>  
</ExcerptHighlights>  
<Summary></Summary>  
<Concepts>  
<string></string>  
</Concepts>  
<CachedDocumentUri></CachedDocumentDocumentUri>  
</QueryResult>  
</Results>  
</QueryResults>

<table>
<thead>
<tr>
<th>Element</th>
<th>Data type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>QueryResults</td>
<td>N/A</td>
<td>Root element.</td>
</tr>
<tr>
<td>Executed</td>
<td>Boolean</td>
<td>True if enough information to perform a search.</td>
</tr>
<tr>
<td>BasicQuery</td>
<td>String</td>
<td>Received BasicQuery parameter content.</td>
</tr>
<tr>
<td>AdvancedQuery</td>
<td>String</td>
<td>Received AdvancedQuery parameter content.</td>
</tr>
<tr>
<td>ExpandedQuery</td>
<td>String</td>
<td>Thesaurus suggested query.</td>
</tr>
<tr>
<td>TotalCount</td>
<td>Integer</td>
<td>Total number of matching documents.</td>
</tr>
<tr>
<td>Time</td>
<td>float</td>
<td>Time required to return results, in seconds.</td>
</tr>
<tr>
<td>Filtered</td>
<td>Boolean</td>
<td>True if duplicate results are filtered. Controlled by the FilterDuplicates parameter.</td>
</tr>
<tr>
<td>Optimized</td>
<td>Boolean</td>
<td>True if query is optimized. Controlled by the Optimize parameter.</td>
</tr>
<tr>
<td>QueryCorrections</td>
<td>N/A</td>
<td>Collection of QueryCorrection elements. Represents the Did You Mean function.</td>
</tr>
<tr>
<td>QueryCorrection</td>
<td>N/A</td>
<td>Contains CorrectedQuery and WordCorrections elements.</td>
</tr>
<tr>
<td>Element</td>
<td>Data type</td>
<td>Description</td>
</tr>
<tr>
<td>----------------------</td>
<td>-----------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>CorrectedQuery</td>
<td>String</td>
<td>Corrected query as if all WordCorrections are applied to BasicQuery.</td>
</tr>
<tr>
<td>WordCorrections</td>
<td>N/A</td>
<td>Collection of WordCorrection elements.</td>
</tr>
<tr>
<td>WordCorrection</td>
<td>N/A</td>
<td>Contains Position, OriginalWord and CorrectedWord elements.</td>
</tr>
<tr>
<td>Position</td>
<td>Integer</td>
<td>Position of OriginalWord in BasicQuery.</td>
</tr>
<tr>
<td>OriginalWord</td>
<td>String</td>
<td>Word that might require a correction.</td>
</tr>
<tr>
<td>CorrectedWord</td>
<td>String</td>
<td>Suggested OriginalWord replacement.</td>
</tr>
<tr>
<td>Results</td>
<td>N/A</td>
<td>Collection of QueryResult elements.</td>
</tr>
<tr>
<td>QueryResult</td>
<td>N/A</td>
<td>Contains UniqueId, Title, TitleHighlights, Uri, PrintableUri, Score, Size, IsAttachment, ContainsAttachment, ModifiedDate, IndexedDate, Fields, IsTopResult, Rating, IsUserRating, LastView, NumberOfViews, Excerpt, and ExcerptHighlights elements.</td>
</tr>
<tr>
<td>UniqueId</td>
<td>Integer</td>
<td>Internal unique document identifier.</td>
</tr>
<tr>
<td>Title</td>
<td>String</td>
<td>Title of the document.</td>
</tr>
<tr>
<td>TitleHighlights</td>
<td>N/A</td>
<td>Collection of Highlight elements.</td>
</tr>
<tr>
<td>Highlight</td>
<td>N/A</td>
<td>Contains Position and Length elements.</td>
</tr>
<tr>
<td>Position</td>
<td>Integer</td>
<td>Position of the expression to highlight in Title.</td>
</tr>
<tr>
<td>Length</td>
<td>Integer</td>
<td>Length of the expression to highlight in Title.</td>
</tr>
<tr>
<td>Uri</td>
<td>String</td>
<td>Address of the document.</td>
</tr>
<tr>
<td>PrintableUri</td>
<td>String</td>
<td>Address that should be displayed to user.</td>
</tr>
<tr>
<td>PrintableUriHighlights</td>
<td>N/A</td>
<td>Collection of Highlight elements.</td>
</tr>
<tr>
<td>Highlight</td>
<td>N/A</td>
<td>Contains Position and Length elements.</td>
</tr>
<tr>
<td>Position</td>
<td>Integer</td>
<td>Position of the expression to highlight in PrintableUri.</td>
</tr>
<tr>
<td>Length</td>
<td>Integer</td>
<td>Length of the expression to highlight in PrintableUri.</td>
</tr>
<tr>
<td>Score</td>
<td>Integer</td>
<td>Relative to the quality of the document in regards of the query.</td>
</tr>
<tr>
<td>Size</td>
<td>Integer</td>
<td>File size in bytes.</td>
</tr>
<tr>
<td>Element</td>
<td>Data type</td>
<td>Description</td>
</tr>
<tr>
<td>----------------------</td>
<td>-----------</td>
<td>------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>IsAttachment</td>
<td>Boolean</td>
<td>True if the file is contained in another file such as a zipped one.</td>
</tr>
<tr>
<td>ContainsAttachment</td>
<td>Boolean</td>
<td>True if contains other files such as a zip.</td>
</tr>
<tr>
<td>ModifiedDate</td>
<td>date/time</td>
<td>Last time the document was modified.</td>
</tr>
<tr>
<td>IndexedDate</td>
<td>date/time</td>
<td>Last time the document was refreshed in the index.</td>
</tr>
<tr>
<td>Fields</td>
<td>N/A</td>
<td>Collection of ResultField elements.</td>
</tr>
<tr>
<td>ResultField</td>
<td>N/A</td>
<td>Contains Name and Value elements.</td>
</tr>
<tr>
<td>Name</td>
<td>String</td>
<td>Name of a field.</td>
</tr>
<tr>
<td>Value</td>
<td>(description)</td>
<td>Value of the field. This element has an attribute xsi:type that denotes the data type of the value.</td>
</tr>
<tr>
<td>IsTopResult</td>
<td>Boolean</td>
<td>True if the document is displayed as a Top Results.</td>
</tr>
<tr>
<td>Rating</td>
<td>float</td>
<td>Document rating in number of stars.</td>
</tr>
<tr>
<td>IsUserRating</td>
<td>Boolean</td>
<td>True if the Rating element denotes that the rating was manually set by the user.</td>
</tr>
<tr>
<td>LastView</td>
<td>date/time</td>
<td>Time when the document was last opened.</td>
</tr>
<tr>
<td>NumberOfViews</td>
<td>Integer</td>
<td>Number of times a document was opened.</td>
</tr>
<tr>
<td>Excerpt</td>
<td>String</td>
<td>Most relevant document excerpt.</td>
</tr>
<tr>
<td>ExcerptHighlights</td>
<td>N/A</td>
<td>Collection of Highlight elements.</td>
</tr>
<tr>
<td>Highlight</td>
<td>N/A</td>
<td>Contains Position and Length elements.</td>
</tr>
<tr>
<td>Position</td>
<td>Integer</td>
<td>Position of the expression to highlight in Excerpt.</td>
</tr>
<tr>
<td>Length</td>
<td>Integer</td>
<td>Length of the expression to highlight in Excerpt.</td>
</tr>
<tr>
<td>Summary</td>
<td>String</td>
<td>Document summary.</td>
</tr>
<tr>
<td>Concepts</td>
<td>N/A</td>
<td>Collection of string elements.</td>
</tr>
<tr>
<td>String</td>
<td>String</td>
<td>One of the most important document words or expressions.</td>
</tr>
<tr>
<td>CachedDocumentUri</td>
<td>String</td>
<td>Address where users can see the document Quick View.</td>
</tr>
</tbody>
</table>

4.9 Integrating the Coveo .NET Search Interface in a Sitecore Website

Integrating the Coveo .NET search interface into Sitecore allows your end-users to search your Coveo index content directly from your Sitecore website using a feature-rich Coveo search interface.

www.coveo.com
Note: If not already done, index the content of your Sitecore site so you can include it in the scope of the search interface to integrate to Sitecore.

To integrate the Coveo search interface in a Sitecore website

1. Using an administrator account, log on to the Sitecore server.
2. If not already done, install or update the Coveo search interfaces on the Sitecore server.
3. Start the IIS Manager (on the Windows taskbar, select Start > Administrative Tools > Internet Information Services (IIS) Manager).
4. In Internet Information Services (IIS) Manager, create a virtual directory for your Sitecore web application:
   a. In the Connections panel, expand to the root of your Sitecore web application, right-click it and select Add Virtual Directory
b. In the Add Virtual Directory dialog box, enter Coveo in the Alias box and the [.NET_Front-End_Path]\Web\Coveo folder in the Physical path box.

5. Using a text editor:
   a. Open the Sitecore web.config file.

   **Note:** It is recommended to make a backup of the web.config file before editing it.

   b. In the configuration\configSections section, add the following code:

```
<sectionGroup name="coveoCnlWeb">
  <section name="customContent" type="System.Configuration.SingleTagSectionHandler, System, Version=1.0.3300.0, Culture=neutral, PublicKeyToken=b77a5c561934e089" />
</sectionGroup>
<configuration name="coveoEnterpriseSearch">
  <section name="database" type="System.Configuration.SingleTagSectionHandler, System, Version=1.0.3300.0, Culture=neutral, PublicKeyToken=b77a5c561934e089" />
  <section name="analytics" type="System.Configuration.SingleTagSectionHandler, System, Version=1.0.3300.0, Culture=neutral, PublicKeyToken=b77a5c561934e089" />
  <section name="locations" type="System.Configuration.SingleTagSectionHandler, System, Version=1.0.3300.0, Culture=neutral, PublicKeyToken=b77a5c561934e089" />
  <section name="server" type="System.Configuration.SingleTagSectionHandler, System, Version=1.0.3300.0, Culture=neutral, PublicKeyToken=b77a5c561934e089" />
</sectionGroup>
```

c. In the configuration\system.web\pages section, add the following code:

```
<controls>
  <add tagPrefix="cnla" namespace="Coveo.CNL.Web.Ajax" assembly="Coveo.CNL.Web, Version=12.0.0.0, Culture=neutral, PublicKeyToken=44110d16825221f2" />
  <add tagPrefix="cnlb" namespace="Coveo.CNL.Web.BetterControls" assembly="Coveo.CNL.Web, Version=12.0.0.0, Culture=neutral, PublicKeyToken=44110d16825221f2" />
  <add tagPrefix="cnlm" namespace="Coveo.CNL.Web.Misc" assembly="Coveo.CNL.Web, Version=12.0.0.0, Culture=neutral, PublicKeyToken=44110d16825221f2" />
  <add tagPrefix="cnlv" namespace="Coveo.CNL.Web.Validators" assembly="Coveo.CNL.Web, Version=12.0.0.0, Culture=neutral, PublicKeyToken=44110d16825221f2" />
  <add tagPrefix="cnlw" namespace="Coveo.CNL.Web.Widgets" assembly="Coveo.CNL.Web, Version=12.0.0.0, Culture=neutral, PublicKeyToken=44110d16825221f2" />
  <add tagPrefix="ces" namespace="Coveo.CES.Web.Search.Controls" assembly="Coveo.CES.Web.Search, Version=12.0.0.0, Culture=neutral, PublicKeyToken=44110d16825221f2" />
</controls>
```
d. In the configuration \configuration\system.web\compilation section, add the following code:

```xml
<assemblies>
  <add assembly="Coveo.CNL, Version=12.0.0.0, Culture=neutral, PublicKeyToken=44110d16825221f2"/>
  <add assembly="Coveo.CNL.Web, Version=12.0.0.0, Culture=neutral, PublicKeyToken=44110d16825221f2"/>
  <add assembly="Coveo.CES.Common, Version=12.0.0.0, Culture=neutral, PublicKeyToken=44110d16825221f2"/>
  <add assembly="Coveo.CES.Web.Search, Version=12.0.0.0, Culture=neutral, PublicKeyToken=44110d16825221f2"/>
</assemblies>
```

e. In the configuration section, add the following code:

```xml
<coveoCnlWeb>
  <customContent uri="/Coveo/" anonymousUri="/Coveo/Anonymous/"/>
  <coveoCnlWeb>
    <coveoEnterpriseSearch>
      <server hostname="localhost" port="52800" servicesHostname="localhost" servicesPort="52810" instance="default" mirrorName="default" sslCertificatePath="C:\Program Files\Coveo .NET Front-End 12\Web\certificate.p12"/>
      <database enabled="false" connectionString="mongodb://localhost/databaseName"/>
      <analytics enabled="false" connectionString="Data Source=yourServerName;Initial Catalog=CoveoAnalytics;Integrated Security=SSPI;"/>
    </coveoEnterpriseSearch>
  </coveoCnlWeb>
</coveoCnlWeb>
```

f. Save the file.

6. Integrate the search interface in a Sitecore layout or sublayout:

   - Add the following code at the appropriate location in the Sitecore .aspx layout or sublayout file in which you want to integrate the Coveo search interface control.

```xml
<%@ Register TagPrefix="ces" Namespace="Coveo.CES.Web.Search.Controls" Assembly="Coveo.CES.Web.Search, Version=12.0.0.0, Culture=neutral, PublicKeyToken=44110d16825221f2" %>
<%@ Assembly Name="Coveo.CNL, Version=12.0.0.0, Culture=neutral, PublicKeyToken=44110d16825221f2" %>
<%@ Assembly Name="Coveo.CNL.Web, Version=12.0.0.0, Culture=neutral, PublicKeyToken=44110d16825221f2" %>
<asp:Panel ID="pnResultsPanel" runat="server">
  <ces:SearchHub id="c" runat="server"/>
</asp:Panel>

OR

a. When you chose to index Sitecore security using a security provider, you must rather add the following code that includes a script to allow the search interface to display the search results corresponding to the currently logged on user.

Using the Sitecore API, the c_OverrideUser script retrieves the currently logged on user and passes this user to the Coveo search Interface.
Note: CES security elements are case sensitive. The Sitecore connector always indexes security elements in lower-case. Ensure to provide a lower-case username for the security to be resolved correctly.

<%@ Control Language="C#" AutoEventWireup="true" Inherits="layouts_PFCEnergy_CoveoSearchResults" Codebehind="CoveoSearchResults.ascx.cs" %>
<%@ Register TagPrefix="ces" Namespace="Coveo.CES.Web.Search.Controls" Assembly="Coveo.CES.Web.Search, Version=12.0.0.0, Culture=neutral, PublicKeyToken=44110d16825221f2" %>
<%@ Assembly Name="Coveo.CNL, Version=12.0.0.0, Culture=neutral, PublicKeyToken=44110d16825221f2" %>
<%@ Assembly Name="Coveo.CNL.Web, Version=12.0.0.0, Culture=neutral, PublicKeyToken=44110d16825221f2" %>
<script runat="server">
void c_OverrideUser(object p_Sender, Coveo.CES.Web.Search.Controls.OverrideUserEventArgs p_Args)
{
    // The name of the security provider defined under the Admin Tool
    string securityProviderName = "Sitecore Security Provider";
    // Get the username from SitecoreAPI
    string userName = Sitecore.Context.GetUserName().ToLower();
    // Add to the collection of identities
    Coveo.CES.Web.Search.Providers.IUserIdentity user = factory.CreateSecurityProviderUser(userName, securityProviderName, false, null);
    p_Args.AdditionalIdentities.Add(user);
}
</script>
<div id="contentMain">
    <asp:Panel ID="pnResultsPanel" runat="server">
        <ces:SearchHub id="c" runat="server" OnOverrideUser="c_OverrideUser"/>
    </asp:Panel>
</div>

Note: OnOverrideUser event is not available for all Coveo search controls such as QuickSearch and SearchBox controls.

The search interface can target an explicit index source as shown in the following script.

<script runat="server">
override void OnInit(EventArgs p_Args)
{
    SearchBinding.MainSearchObject.SetupSearchBuilder += this.Search_SetupSearchBuilder;
    base.OnInit(p_Args);
}

void Search_SetupSearchBuilder(object p_Sender, SetupSearchBuilderEventArgs p_Args)
{
    p_Args.Builder.AddConstantExpression("@Source=MySourceName");
}
</script>

7. Using a browser, access the modified page to view the search hub.

The Front-End Server Configuration first time setup page appears to allow you to complete the Coveo Front-End installation.
Tip: If you notice that some of Coveo images or JavaScript are missing because they do not load in the search interface, you can fix this problem with a simple edit of the Sitecore web.config file (not the Coveo web.config file). In the file, locate the <setting name="IgnoreUrlPrefixes"...> tag and add the /Coveo/ string to the value attribute.

Example:

```xml
<setting name="IgnoreUrlPrefixes"
value="/sitecore/default.aspx|/trace.axd|/webresource.axd|/Coveo/"/>
```

What's Next?

Consider also integrating the Coveo search in the Sitecore Content Editor (see "Integrating the Coveo .NET Search in the Sitecore Content Editor" on page 163).

4.10 Integrating the Coveo .NET Search in the Sitecore Content Editor

You can integrate the Coveo .NET search interfaces in your Sitecore website to provide a better search experience to your website users (see "Integrating the Coveo .NET Search Interface in a Sitecore Website" on page 158).

You can also integrate the Coveo search in the Sitecore Content Editor so that people contributing to the site content can also take advantage of the Coveo search features and more easily find information in the whole content, not just published content.

**Note:** The integration described in this topic works with Coveo .NET Front-End 12.0.61+.  

Tip: Typically, a Sitecore site is managed with a Master database containing the whole content and a Web database containing only the published content. You can create separate sources for these two databases, and then assign the Web source to the scope of the search interface integrated in the website, and the Master source to the scope of the search interface integrated in the Content Editor. This way, all of the unpublished content is searchable from the Sitecore Desktop.

To integrate the Coveo search in the Sitecore Content Editor

1. If not already done, install the Coveo Front-End components on your Sitecore server.
2. Install the Coveo Content Search for Sitecore:
a. Log in to the Sitecore Desktop user interface using an administrative account.

c. In the **Installation Wizard** dialog box:
   i. In the **Welcome to the Install Package Wizard** screen, click **Next**.
   ii. In the **Select Package** screen:
      i. Click **Upload**, and then browse the Coveo Master server to select the Coveo Content Search package distributed with CES:

      ![Installation Wizard](image)

      ```
      [CES_Install_Path]\Bin\Sitecore6.0CoveoContentSearch2.zip
      
      **Note:** Use the `Sitecore6.0CoveoContentSearch.zip` package only when you use the Sitecore legacy connector.
      ```
      ii. Click **Next**.
   
      iii. In the **Ready to Install** screen, click **Install**.

      **Note:** If an Access Denied error is displayed for the `bin_install` folder while installing the package, verify the security permissions for `ASP.NET` in the bin folder of Sitecore or install the files manually.

   d. Select the **Restart the Sitecore client** option, and then click **Finish**.

3. Using an administrator account, connect to your Sitecore server.

4. Create the Coveo virtual directory:
   a. Open IIS.
   
   b. In IIS, locate and right-click the website that corresponds to your Sitecore instance, and then select **Add virtual directory**.
   
   c. In the **Create Virtual Directory** dialog box:
      i. In the **Alias** box, enter Coveo.
      
      ii. In the **Physical path** box, enter `\.[NET_Front-End_Path]\Web\Coveo`, typically `C:\Program Files\Coveo .NET Front-End 12\Web\Coveo`.

   d. Close IIS.
5. Using a text editor, edit the Sitecore web.config file:

**Example:** For an instance named Sitecore, the file is located in the
C:\inetpub\wwwroot\Sitecore\WebSite folder.

a. Copy the following code and paste it just before the `</configSections>` tag.

```xml
<sectionGroup name="coveoCnlWeb">
  <section name="customContent" type="System.Configuration.SingleTagSectionHandler, System, Version=1.0.3300.0, Culture=neutral, PublicKeyToken=b77a5c561934e089" />
</sectionGroup>
<sectionGroup name="coveoEnterpriseSearch">
  <section name="database" type="System.Configuration.SingleTagSectionHandler, System, Version=1.0.3300.0, Culture=neutral, PublicKeyToken=b77a5c561934e089" />
  <section name="analytics" type="System.Configuration.SingleTagSectionHandler, System, Version=1.0.3300.0, Culture=neutral, PublicKeyToken=b77a5c561934e089" />
  <section name="locations" type="System.Configuration.SingleTagSectionHandler, System, Version=1.0.3300.0, Culture=neutral, PublicKeyToken=b77a5c561934e089" />
  <section name="server" type="System.Configuration.SingleTagSectionHandler, System, Version=1.0.3300.0, Culture=neutral, PublicKeyToken=b77a5c561934e089" />
</sectionGroup>
```

b. Copy the following code and paste it just before the `</controls>` tag, a child of the `<pages>` tag.

```xml
<add tagPrefix="cnla" namespace="Coveo.CNL.Web.Ajax" assembly="Coveo.CNL.Web, Version=12.0.0.0, Culture=neutral, PublicKeyToken=44110d16825221f2"/>
<add tagPrefix="cnlb" namespace="Coveo.CNL.Web.BetterControls" assembly="Coveo.CNL.Web, Version=12.0.0.0, Culture=neutral, PublicKeyToken=44110d16825221f2"/>
<add tagPrefix="cnlm" namespace="Coveo.CNL.Web.Misc" assembly="Coveo.CNL.Web, Version=12.0.0.0, Culture=neutral, PublicKeyToken=44110d16825221f2"/>
<add tagPrefix="cnlw" namespace="Coveo.CNL.Web.Widgets" assembly="Coveo.CNL.Web, Version=12.0.0.0, Culture=neutral, PublicKeyToken=44110d16825221f2"/>
```

c. Copy the following code and paste it just before the `</namespace>` tag, a child of the `<namespaces>` tag.

```xml
<add namespace="Coveo.CES.Web.Search"/>
<add namespace="Coveo.CES.Web.Search.Controls"/>
<add namespace="Coveo.CNL.Web"/>
```

d. Copy the following code and paste it just before the `</assemblies>` tag, a child of the `<compilation>` tag.

```xml
<add assembly="Coveo.CNL, Version=12.0.0.0, Culture=neutral, PublicKeyToken=44110d16825221f2"/>
<add assembly="Coveo.CES.Common, Version=12.0.0.0, Culture=neutral, PublicKeyToken=44110d16825221f2"/>
<add assembly="Coveo.CNL.Web, Version=12.0.0.0, Culture=neutral, PublicKeyToken=44110d16825221f2"/>
<add assembly="Coveo.CES.Web.Search, Version=12.0.0.0, Culture=neutral, PublicKeyToken=44110d16825221f2"/>
```

e. Copy the following code and paste it at the end of the file, just before the `</configuration>` tag.
f. Save the file.

6. When CES and Sitecore are not installed on the same server, copy the index certificate file from the Coveo Master server to the Sitecore server:
   a. Using an administrator account, connect to the Coveo Master server.
   b. Copy the index certificate file [Index_Path] Config Certificates cert-iis.p12, typically C:\CES7\Config\Certificates\cert-iis.p12.
   c. Paste the certificate file on the Sitecore server into the Sitecore instance website.

Example: For an instance named Sitecore, the default path is C:\inetpub\wwwroot\Sitecore\Website. You can also rename the certificate file such as ces-certificate.p12.

7. Configure the connection to the CES index. Using a text editor:
   a. Open the Sitecore instance web.config file.
   b. Under the <coveoEnterpriseSearch> tag, edit the <server> tag to include the following attributes:
      - hostname=""MyCoveoMasterServerHostName" where you replace MyCoveoMasterServerHostName with the name of your Coveo Master server or localhost when CES and Sitecore are on the same machine.
      - sslCertificatePath="C:\inetpub\wwwroot\Sitecore\Website\ces-certificate.p12", ensuring that the path points to your certificate file.
      - port="52800", the default CES port number.

Example: When CES and Sitecore are on the same server.

<server hostname="localhost" port="52800" servicesHostname="localhost" servicesPort="52810" instance="default" mirrorName="default" sslCertificatePath="C:\Program Files\Coveo .NET Front-End 12\Web\ces-certificate.p12"/>

8. Configure the Sitecore source used by Coveo search:
   a. Using a text editor, open the CoveoSearch.aspx file.

Example: For a Sitecore instance named Sitecore, the file is typically located in the C:\inetpub\wwwroot\Sitecore\Website\sitecore\shell\Applications\Coveo\ folder.

b. Locate the following code:
and replace it with:

```csharp
p_Args.Builder.AddConstantExpression("@Source=""YOUR SITECORE SOURCE NAME HERE"";
```

where you replace YOUR SITECORE SOURCE NAME HERE by the name of the source you created to contain the whole Sitecore content, typically indexing the master database.

c. Save and close the file.

### 4.11 Enabling Anonymous Access to a .NET Search Interface

The Coveo Platform search interfaces are typically deployed within an enterprise firewall. You can also deploy Coveo .NET search interfaces on public facing websites and allow anonymous users to view search results.

**Example:** When Coveo is integrated in a public Sitecore website, anonymous users accessing the website should be able to see search results for publicly available content.

To configure a public facing .NET search interface

1. When your Coveo index contains non public sources, ensure that the scope of the .NET search interfaces that are publicly exposed includes only sources with content that should appear in public search results.

   When using the out-of-the-box Coveo .NET search interfaces, you can configure the scope from the .NET Interface Editor.

2. In IIS on the web server:
   a. Select the Coveo search website (by default Coveo .NET Front-End 12).
   b. Click **Authentication** and then set:
      - **Anonymous Authentication** to Enabled
      - **Windows Authentication** to Disabled

3. Reset IIS to make the changes take effect.

   **Note:** All websites on the server will be temporarily unavailable.

4. Access the Coveo Administration Tool.

5. In the Administration tool, for each source included in your public facing .NET search interface:
   a. In the **Permissions** page under **Custom Permissions**:
      - Add the **nt authority\anonymous logon** Active Directory group to the **Allowed Users** list.
      **Note:** When you also want authenticated users to also see all anonymous search results, you must
also add the user that runs the application of the website in the permission of the source.

- Remove the **everyone** Active Directory group from the **Allowed Users** list.

b. Click **Rebuild** to rebuild the source.

### 4.12 Creating a Custom Color Scheme for the Desktop Searchbar in the Windows Registry

**Deprecated**

**Desktop Integration Package 12.0.316+ (October 2013)**

End-users can select an out-of-the-box predefined color scheme for the Desktop Searchbar. It is also possible to create a custom color scheme for the Desktop Searchbar, for example to match your organization official colors.
Note: Desktop Integration Package 12.0.1888+ (September 2016) You can create custom color schemes in a JSON file stored on the web server from which the DIP gets results, without requiring your end-users to create registry keys on their machine.

For search interfaces powered by Coveo .NET Front-End, create and refer to the file containing the color schemes in the DIP JSON configuration file (see Customizing Desktop Integration Package (DIP) Bitmaps and Colors).

To create a custom color scheme for the Desktop Searchbar in the Windows registry

1. Log in to a computer on which the Desktop Integration Package is installed.
2. Turn off the Desktop Integration Package by selecting the contextual menu of the Coveo Desktop Integration Package system icon , and then selecting Exit in the contextual menu.
3. Open the Windows Registry Editor (by pressing the Windows+r keys, and then typing regedit).
4. In the Registry Editor:
   a. Search or navigate to HKEY_CURRENT_USER > Software > Coveo > Search Bar > SearchBarScheme.
   b. Right-click SearchBarScheme, and then select New > Key.
   c. In the new folder, enter a name for your new color scheme. This name however is not the color scheme name that the end-user will see.
   d. Right-click the new folder, select New > String Value, and create each of the string values described in the following table.

<table>
<thead>
<tr>
<th>Name</th>
<th>Value (example)</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default</td>
<td>0</td>
<td>Set to 1 to make this scheme the default scheme. &lt;br&gt;<strong>Important:</strong> Only one scheme must be the default theme otherwise the DIP will not start.</td>
</tr>
<tr>
<td>My Theme</td>
<td>My Theme</td>
<td>The scheme name visible to the end-user in the Predefined color scheme drop-down list in the DIP options. Do not enclose the name between {}.</td>
</tr>
<tr>
<td>SearchbarBackgroundResultColor</td>
<td>#C8C8C8</td>
<td>Search results background color</td>
</tr>
<tr>
<td>SearchbarBackgroundSearchColor</td>
<td>#E1E1E1</td>
<td>Search section background color</td>
</tr>
</tbody>
</table>

Tip: You can start with colors from one of the out-of-the-box color schemes (see "Default Desktop Searchbar Color Schemes" on page 171).
5. Restart the DIP by selecting the Windows Start button, typing Coveo Search Bar, and then pressing Enter.

6. From the DIP options, select the newly created color scheme.

7. Validate that the scheme appears as expected.

4.12.1 Default Desktop Searchbar Color Schemes

The following table presents the Registry Editor values for the default HKEY_CURRENT_USER > Software > Coveo > Search Bar > SearchBarScheme Desktop Searchbar color schemes (see "Creating a Custom Color Scheme for the Desktop Searchbar in the Windows Registry" on page 169).

<table>
<thead>
<tr>
<th>Registry string name</th>
<th>Registry string value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Black</td>
<td>0</td>
</tr>
<tr>
<td>Light blue</td>
<td>#8C8C8C</td>
</tr>
<tr>
<td>Blue</td>
<td>#F3F3F3</td>
</tr>
<tr>
<td>Light gray</td>
<td>#DADEE</td>
</tr>
<tr>
<td>Gray</td>
<td>#F3F3F3</td>
</tr>
<tr>
<td>Light orange</td>
<td>#F3F3F3</td>
</tr>
<tr>
<td>Orange</td>
<td>#FFCA9B</td>
</tr>
</tbody>
</table>

SearchbarBackgroundColorResultColor
- #C8C8C8 | #F3F3F3 | #CFDEE | #F3F3F3 | #DADEE | #F3F3F3 | #FFCA9B

SearchbarBackgroundColorSearchColor
- #E1E1E1 | #EBF5F5 | #E7F1F1 | #E2E2E2 | #DADEE | #E2E2E2 | #F8F8F8 | #FFECD |

SearchbarCloseButtonBorderColor
- #ABABAB | #ABABAB | #ABABAB | #ABABAB | #ABABAB | #ABABAB | #ABABAB | #ABABAB
### 4.13 Creating a Custom Color Scheme for the Outlook Sidebar in the Windows Registry

**Deprecated**

**Desktop Integration Package 12.0.316+ (October 2013)**

End-users can select an out-of-the-box predefined color scheme for the Outlook Sidebar. It is also possible to create a custom color scheme for the Outlook Sidebar, for example to match your organization official colors.

#### Note: Desktop Integration Package 12.0.1888+ (September 2016)

You can create custom color schemes in a JSON file stored on the web server from which the DIP gets results, without requiring your end-users to create registry keys on their machine.

For search interfaces powered by Coveo .NET Front-End, create and refer to the file containing the color schemes in the DIP JSON configuration file (see Customizing Desktop Integration Package (DIP) Bitmaps and Colors).

To create a custom color scheme for the Outlook Sidebar in the Windows registry:

1. Log in to a computer on which the Desktop Integration Package is installed.
2. Close Outlook.
3. Turn off the Desktop Integration Package by selecting the contextual menu of the Coveo Desktop Integration.
Package system icon, and then selecting Exit in the contextual menu.

4. Open the Windows Registry Editor (by pressing the Windows+r keys, and then typing regedit).

5. In the Registry Editor:
   a. Search or navigate to HKEY_CURRENT_USER > Software > Coveo > Search Bar > OutlookScheme.
   b. Right-click OutlookScheme, and then select New > Key.
   c. For the new folder, enter a name for your new color scheme. This name however is not the color scheme name that the end-user will see.
   d. Right-click the new folder, select New > String Value, and create each of the string values described in the following table.

<table>
<thead>
<tr>
<th>Name</th>
<th>Value (example)</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default</td>
<td>0</td>
<td>Set to 1 to make this scheme the default scheme.</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Important:</strong> Only one scheme must be the default theme otherwise the DIP will not start.</td>
</tr>
<tr>
<td>My Theme</td>
<td></td>
<td>The scheme name visible to the end-user in the Predefined color scheme drop-down list in the DIP options. Do not enclose the name between {}.</td>
</tr>
<tr>
<td>GripColor</td>
<td></td>
<td>Color of the bar used to resize the number of available search interface tabs.</td>
</tr>
<tr>
<td>GripPointsColor</td>
<td></td>
<td>Color of the three dots in the bar used to resize the number of available search interface tabs.</td>
</tr>
<tr>
<td>MainColor</td>
<td></td>
<td>Main Sidebar color</td>
</tr>
<tr>
<td>OutlookTheme</td>
<td></td>
<td>Leave this string empty. Used only for out-of-the-box schemes.</td>
</tr>
<tr>
<td>SearchButtonColor</td>
<td></td>
<td>Search button color</td>
</tr>
<tr>
<td>SearchButtonColorPressed</td>
<td></td>
<td>Search button color when pressed.</td>
</tr>
<tr>
<td>SidebarBorderColor</td>
<td></td>
<td>Color of the vertical bar used to resize the Sidebar.</td>
</tr>
<tr>
<td>TabColor</td>
<td></td>
<td>Tab text color when not selected neither hovered.</td>
</tr>
<tr>
<td>TabSelectedColor</td>
<td></td>
<td>Tab text color when selected.</td>
</tr>
<tr>
<td>TabHoveredColor</td>
<td></td>
<td>Tab text color when hovered.</td>
</tr>
</tbody>
</table>
6. Restart the DIP by selecting the Windows Start button, typing Coveo Search Bar, and then pressing Enter.

7. Restart Outlook.

8. From the DIP options, select the newly created color scheme.

9. Validate that the scheme appears as expected.

4.14 Microsoft SharePoint Integration

Coveo search boxes and Coveo .NET Front-End search interfaces can be integrated into SharePoint to allow SharePoint users to get Coveo powered search results directly into SharePoint. The .NET search interfaces outside SharePoint can also be configured to show secured SharePoint results for various types of user authentication without users having to sign on again.

4.14.1 Integrating the Coveo .NET Search Box in My Site for SharePoint 2013 and 2016

You can replace the Microsoft search box by the Coveo .NET search box for the My Site pages. On each SharePoint 2013 and 2016 front-end server, perform the following procedure to edit the template that applies the changes to the My Site page for all users.

To integrate the Coveo .NET search box in all My Site pages

1. Using an administrator account, log in to the SharePoint 2013 or 2016 front-end server.

2. Enable the Coveo Search Box feature for the My Site pages (see "Activating or Deactivating the Coveo .NET Search Box in a SharePoint Site" on page 176).

   **Note:** Enabling the Coveo Search Box feature from My Site will not enable it for other pages.

   **Example:** To replace the search boxes in the Home page, you must enable the Coveo Search Box feature when you click on the Site Setting while being on the Home page.

With SharePoint 2013, enabling the Coveo Search Box feature will unfortunately not be enough to replace all the Microsoft default search boxes in My Site. You also need to modify three files as described in the following steps.
3. **Using a text editor, open the** C:\Program Files\Common Files\Microsoft Shared\Web Server Extensions\15\TEMPLATE\FEATURES\MySiteUnifiedNavigation\mysite15.master** file, and then:**

   a. **At the beginning of the file, after the last existing `<%@ Register TagPrefix="...` line, add the following line:**

   ```
   <%@ Register TagPrefix="cessp" Namespace="Coveo.CES.Web.Search.SharePoint.Controls"
   Assembly="Coveo.CES.Web.Search.SharePoint, Version=12.0.0.0, Culture=neutral,
   PublicKeyToken=44110d16825221f2" %>
   ```

   b. **Towards the end of the file, replace the following code segment:**

   ```
   <div id="searchInputBox">
   <SEARCHWC:SearchBoxScriptWebPart runat="server" id="searchInputBox"
   DefaultDropdownNodeId="1001" ServerInitialRender="true" UseSharedSettings="true"
   ChromeType="none" EmitStyleReference="false"/>
   </div>
   ```

   **with the following code segment:**

   ```
   <div id="searchInputBox">
   <cessp:SharePointSearchBox runat="server"/>
   </div>
   ```

   c. **Save the file.**

4. **Using a text editor, open the** C:\Program Files\Common Files\Microsoft Shared\Web Server Extensions\15\TEMPLATE\SiteTemplates\SPSMSITEHOST\default.aspx** file (default location), and then:**

   a. **At the beginning of the file, after the last existing `<%@ Register TagPrefix="...` line, add the following line:**

   ```
   <%@ Register TagPrefix="cessp" Namespace="Coveo.CES.Web.Search.SharePoint.Controls"
   Assembly="Coveo.CES.Web.Search.SharePoint, Version=12.0.0.0, Culture=neutral,
   PublicKeyToken=44110d16825221f2" %>
   ```

   b. **Towards the end of the file, replace the following code segment:**

   ```
   <div id="searchInputBox" class="ms-mpSearchBox ms-mysite-searchBox">
   <SEARCHWC:SearchBoxScriptWebPart runat="server" id="searchInputBox"
   DefaultDropdownNodeId="1003" ServerInitialRender="true" UseSharedSettings="true"
   ChromeType="none" EmitStyleReference="false"/>
   <SPSWC:MySiteSearchBoxDefaultOverride DefaultId="1003" runat="server"/>
   </div>
   ```

   **with the following code segment:**

   ```
   <div id="searchInputBox" class="ms-mpSearchBox ms-mysite-searchBox">
   <cessp:SharePointSearchBox runat="server"/>
   </div>
   ```

   c. **Save the file.**

5. **Using a text editor, open the** C:\Program Files\Common Files\Microsoft Shared\Web Server Extensions\15\TEMPLATE\FEATURES\SocialDataStore\SocialDataStoreList\sites.aspx** file (default location), and then:**
a. At the beginning of the file, after the last existing `<%@ Register TagPrefix="..." line, add the following line:

```coveo
<%@ Register TagPrefix="cessp" Namespace="Coveo.CES.Web.Search.SharePoint.Controls"
Assembly="Coveo.CES.Web.Search.SharePoint, Version=12.0.0.0, Culture=neutral,
PublicKeyToken=44110d16825221f2" %>
```

b. Towards the end of the file, replace the following code segment:

```coveo
<div class="ms-contentFollowing-searchBox ms-tableCell ms-verticalAlignTop">
<SEARCHWC:SearchBoxScriptWebPart runat="server" id="searchInputBox"
DefaultDropdownNodeId="1001" ServerInitialRender="true" UseSharedSettings="true"
ChromeType="none" EmitStyleReference="false"/>
</div>
```

with the following code segment:

```coveo
<div class="ms-contentFollowing-searchBox ms-tableCell ms-verticalAlignTop">
<cessp:SharePointSearchBox runat="server" />
</div>
```

c. Save the file.

6. Reload the My Site page of a user to verify that the Coveo search box is now appearing in the top navigation section of the page.

7. Repeat the procedure for each SharePoint 2013 or 2016 front-end server.

4.14.2 Activating or Deactivating the Coveo .NET Search Box in a SharePoint Site

Once you installed the Coveo .NET search box on a SharePoint server (see "Installing the Coveo Web Service, Search Box, and Search Interface into SharePoint" on page 1309), you can activate/deactivate the Coveo .NET search box independently for each SharePoint site.

---

**Note:** SharePoint 2016/2013/2010/2007 offers a mechanism, called DelegateControl that allows administrators to replace controls displayed in SharePoint pages. The Microsoft search box and scope selector are in the same DelegateControl called SmallSearchInputBox. The Coveo installer deploys a feature called CoveoSearchBox to replace the Microsoft controls in the SmallSearchInputBox.

To activate or deactivate the Coveo .NET search box in a SharePoint 2013 and 2016 site

1. Using a browser, access the SharePoint site into which you want to change the state of the Coveo search box.

   **Note:** You can activate the Coveo Search Box feature on any of the four SharePoint levels (Farm, WebApp, SiteCollection, and Site). Ensure to activate the Coveo search box everywhere you want it to replace the Microsoft default search boxes.

   **Example:** Activate the Coveo search box feature at the Farm level, to activate it all over your SharePoint installation.

2. On the Gear menu, select Site Settings.
3. In the page that appears, under **Site Collection Administration**, click **Site collection features**.

4. In the **Site Settings > Site Collection Features** page, locate **Coveo Site Collection Search**, and then click **Activate** or **Deactivate** on the corresponding line.

To activate or deactivate the Coveo search box in a SharePoint 2010 site

1. Using a browser, access the SharePoint site into which you want to change the state of the Coveo search box.

   **Note:** You can activate the **Coveo Search Box** feature on any of the four SharePoint levels (Farm, WebApp, SiteCollection, and Site). Ensure to activate the Coveo search box everywhere you want it to replace the Microsoft default search boxes.

   **Example:** Activate the Coveo search box feature at the Farm level, to activate it all over your SharePoint installation.

2. On the **Site Actions** menu, select **Site Settings**.

3. In the **Site Settings** page, under **Site Collection Administration**, click **Site collection features**.

4. In the **Site Collection Administration > Features** page, locate **Coveo Site Collection Search**, and then click
4.14.3 Manually Configuring a .NET Search Interface Claims SSO for an On-Premises SharePoint

A Coveo .NET Front-End search interface that resides outside SharePoint must authenticate the SharePoint end-user performing the query to return SharePoint search results for which the end-user has read access in SharePoint. No SharePoint results are returned to unauthenticated users.

**Note:** Coveo .NET Front-End 12.0.1548+ (June 2016) The procedure described in this topic is no longer needed with the new Coveo Front-end SSO Configuration page.

This topic describes how to configure both your SharePoint server and your Coveo .NET Front-End to provide a single sign on (SSO) solution and automatically authenticate Claims end-users in a Coveo .NET search interface that reside outside SharePoint.

You can provide this seamless experience to end-users searching for secured content indexed from Claims-enabled SharePoint web applications using Windows authentication (NTLM) even when your SharePoint environment does not use the Windows Identity Foundation (WIF).

**How it Works**

The Coveo SSO solution uses browser redirections similar to what the Windows Identity Foundation (WIF) does to authenticate users with Claims-aware web applications:

- A user accesses the Coveo .NET search interface with a browser.
- When the Coveo SharePoint Claims cookie is not available or expired, the Coveo search interface web app redirects the browser to a Coveo deployed specific web page on the SharePoint server.
- This SharePoint web page uses NTLM or Kerberos so it can retrieve the full Claims identities of the user or otherwise prompts the user to login to SharePoint.
The SharePoint web page encrypts, packages, and sends the Claims back to the Coveo search interface web app.

The Coveo search interface web app receives the user Claims package, creates the cookie, and reloads the Coveo search interface page.

The user now has the full Claims identities to perform his queries.

The round trip may or may not be noticeable depending on your environment.

**HTTPS Versus HTTP**

You can configure Claims SSO for both secure (HTTPS) and non-secure (HTTP) connections. When a Coveo search page or a SharePoint web application can be accessed from outside a firewall (Internet), HTTPS is recommended. When Coveo and SharePoint servers can be accessed only from client machines running behind the same firewall, both HTTP and HTTPS are good options. The examples presented in this topic arbitrarily show HTTPS connections.

When the claims authentication is enabled between a Coveo Front-End and a SharePoint web application, tokens are exchanged between both servers. A token basically contains the user identity, but never contains passwords or other sensitive information. The tokens are encoded, compressed, and signed, to prevent an eventual hacker from altering and using them illegitimately.

**Note:** Coveo .NET Front-End 12.0.614 to 12.0.844 (February to June 2014) Claims SSO can be configured only for secure (HTTPS) connections.

### 4.14.3.1 SharePoint Server Configuration

**Note:** When you have more than one SharePoint front-end server in your SharePoint farm, you must perform the following procedure for each SharePoint front-end server.

1. Ensure that your environment meets the following requirements:
   - SharePoint 2013/2010 (on-premises)
   - SharePoint server web application configured in Windows Claims (NTLM or Kerberos)

2. Coveo .NET Front-End 12.0.614+ (February 2014)

2. Using an administrator account, connect to the operating system of your SharePoint front-end server.

3. If not already done, deploy the Coveo integration in your SharePoint web application to ensure that at least the SharePoint Web Service option is installed (see "Installing the Coveo Web Service, Search Box, and Search Interface into SharePoint" on page 1309).

4. On the first front-end server of your SharePoint farm, create two empty files that will be filled with the private and public communication signing keys.

**Note:** The private and public keys are generated by the front-end server at the first use. You can easily regenerate new keys simply by deleting the original key files and recreating these two empty files.
On other front-end servers of your SharePoint farm, rather paste a copy of these filled files (do not copy the empty files) to ensure that all front-end servers use the same public and private key files.

**Example:** The files could be:

- `C:\Program Files\Coveo .NET Front-End 12\Web\ClaimsAuthenticationKeys\ClaimsAuthenticationPublicKey.bin`
- `C:\Program Files\Coveo .NET Front-End 12\Web\ClaimsAuthenticationKeys\ClaimsAuthenticationPrivateKey.bin`

**Important:** Protect your private key file once it is created. This file should never be shared nor sent via email. Anyone that can access this key could use it to create his own Claims and be able to gain access to all SharePoint documents from CES.

5. Right-click the key file folder and then use its **Properties** to ensure that the application pool identity running the web application where Coveo is integrated has read and write access to the key files.

6. Using a text editor:
   a. Open the `web.config` file of the SharePoint web application site.

   **Example:** The file is typically:

   ```
   C:\inetpub\wwwroot\wss\VirtualDirectories\12345\web.config
   ```

   b. **Under** `coveoEnterpriseSearch`, if not already present, add a `claimsAuthentication` section, ensure it includes the following attributes, and then update the attributes values according to your setup:

   ```
   - identityReceiverUrl="https://YourCoveoFrontEnd/ClaimsIdentityReceiver.aspx"
   - identityProviderPrivateKeyPath="PathToPrivateKey"
   - identityProviderPublicKeyPath="PathToPublicKey"
   ```

   **Example:** The `claimsAuthentication` section looks like:

   ```
   <claimsAuthentication
   identityReceiverUrl="https://YourCoveoFrontEnd/ClaimsIdentityReceiver.aspx"
   identityProviderPrivateKeyPath="C:\Program Files\Coveo .NET Front-End 12\Web\ClaimsAuthenticationKeys\ClaimsAuthenticationPrivateKey.bin"
   identityProviderPublicKeyPath="C:\Program Files\Coveo .NET Front-End 12\Web\ClaimsAuthenticationKeys\ClaimsAuthenticationPublicKey.bin"/>
   ```

   c. **Coveo .NET Front-End 12.0.1459+ (March 2016)** When the search page is accessed via a Network Load Balancing (NLB) IP address, just before `<coveoEnterpriseSearch>`, you may have to add the `assumedHttpRequestUrlScheme` option in the following format:

   ```
   <options assumedHttpRequestUrlScheme="value"/>
   ```

   replacing `value` by either `http` or `https`. 
Important: If missing, you must add the following element before the closing sectionGroup tag \(</sectionGroup>\) for the assumedHttpRequestUrlScheme option to be supported:

\(<\text{section name=\"options\" type=\"System.Configuration.SingleTagSectionHandler, System, Version=1.0.3300.0, Culture=neutral, PublicKeyToken=b77a5c561934e089\" />>

Notes:

- When the option is present, the .NET UI assumes that the search page is always opened using the specified scheme. Otherwise, the .NET UI assumes IIS detects the right scheme.
- You may also have to add the option in the Coveo .NET Front-End web.config file (see Coveo .NET Front-End Server Configuration).
- You can use this option when troubleshooting the Coveo.CES.Web.Search.Security.ClaimsIdentityException: Attempt to retrieve a token in HTTP without supplying the main identity. error.

Example: Your IIS site is configured to switch automatically in HTTPS if a browser tries to open the search page in HTTP, so you add \(<\text{options assumedHttpRequestUriScheme=\"https\"} />\).

d. If more than one standalone Coveo Front-End server use this SharePoint web application as their identity provider or if the standalone Coveo front-end server can be reached from multiple URLs, in the \(<\text{identityReceivers}\) subsection, configure each one to allow them to retrieve the cookie.

Example:

\(<\text{claimsAuthentication}\
\text{identityReceiverUri=\"https://DefaultCoveoFrontEnd/ClaimsIdentityReceiver.aspx\"}\
\text{identityProviderPrivateKeyPath=\"PathToPrivateKey\"}\
\text{identityProviderPublicKeyPath=\"PathToPublicKey\"}\
\text{<identityReceivers}}\n\quad\text{<add domain=\"CoveoFrontEnd1\" url=\"https://CoveoFrontEnd1/ClaimsIdentityReceiver.aspx\"} />\n\quad\text{<add domain=\"CoveoFrontEnd1DifferentUrl\" url=\"https://CoveoFrontEnd1DifferentUrl/ClaimsIdentityReceiver.aspx\"} />\n\quad\text{<add domain=\"CoveoFrontEnd2\" url=\"https://CoveoFrontEnd2/ClaimsIdentityReceiver.aspx\"} />\n\text{</identityReceivers>}}\n\text{</claimsAuthentication>}

Notes:

- Coveo .NET Front-End 12.0.777+ (May 2014) The \(<\text{identityProviders}\) subsection is supported.
- You should also leave a working identity receiver URL in the \(<\text{claimsAuthentication}\) section that will be used when the user comes from another domain.

e. Save the file.

7. Using a browser, access to the URL of the following form to test your setup:

https://YourSharePointSite/_layouts/CES/ClaimsIdentityProvider.aspx?debug=1

You should see a web page that contains various claims information. You should not see errors. The private and public key files should now be filled with the new key data.

8. At this point, if you want, you can remove the write access of the web application pool identity to the key files.
4.14.3.2 Coveo .NET Front-End Server Configuration

**Note:** When you have more than one Coveo Front-End server in your Coveo deployment, you must perform the following procedure for each Coveo Front-End server.

1. Using an administrator account, connect to the operating system of your Coveo .NET Front-End server.

2. Copy the public key file created on your SharePoint front-end server and paste it to the Coveo Front-End server.

   **Example:** On the Coveo .NET Front-End server, you can copy the file to:
   
   C:\Program Files\Coveo .NET Front-End 12\Web\ClaimsAuthenticationKeys\ClaimsAuthenticationPublicKey.bin

   **Note:** The public key file does not have to be secured like the private key file. It can safely be shared on a file share or sent by email.

3. Using a text editor:
   a. Open the Coveo .NET Front-End web.config file.

      **Example:** The file is typically:
      
      C:\Program Files\Coveo .NET Front-End 12\Web\Web.config

   b. Under coveoEnterpriseSearch, if not already present, add a claimsAuthentication section, and ensure it includes the following attributes, and then update the attributes values according to your setup:

      - identityProviderUrl="https://YourSharePointSite/_layouts/CES/ClaimsIdentityProvider.aspx"
      - identityValidatorPublicKeyPath="PathToPublicKey"

      **Example:** The claimsAuthentication section looks like:
      
      `<claimsAuthentication identityProviderUrl="https://YourSharePointSite/_layouts/CES/ClaimsIdentityProvider.aspx" identityValidatorPublicKeyPath="C:\Program Files\Coveo .NET Front-End 12\Web\ClaimsAuthenticationKeys\ClaimsAuthenticationPublicKey.bin"/>

   c. **Coveo .NET Front-End 12.0.1459+ (March 2016)** When you add the assumedHttpRequestUriScheme option in the web.config file of the SharePoint web application site, just before </coveoEnterpriseSearch>, specified the same option and value.

      **Example:** Your IIS site is configured to switch automatically in HTTPS if a browser tries to open the search page in HTTP, so you add (<options assumedHttpRequestUriScheme="https" />).

   d. If not already present, as shown in the following file sample, add the Coveo.CES.Web.Search.Security
namespace.

```xml
<configuration>
  <system.web>
    <pages>
      <namespaces>
        ...
        ...
      </namespaces>
    </pages>
  </system.web>
</configuration>
```

**Note:** CES 7.0.6339 – (January 2014) You need at least two CES upgrades subsequent to the CES 7.0.6424 (February 2014 monthly release) or a fresh install of the Coveo .NET Front-End to see the Coveo.CES.Web.Search.Security namespace.

e. Save the file.

4. Using a browser, access your Coveo .NET search interface using the real hostname of the server, not localhost.

Example: The Coveo .NET search interface page URL is typically:

https://YourCoveoFrontEndServer/

The first time you access the .NET search interface with a given browser, a security cookie is created (see "How it Works" on page 178).

**Note:** When your SharePoint server is configured to prompt the users for a password, the user will have to enter its SharePoint password in the process.

5. Perform the first-time setup to configure the Coveo .NET Front-End (see "Coveo .NET Front-End First Time Setup" on page 47).

6. In the Coveo .NET search interface, verify that you have access to all your secured SharePoint documents. When the scope of the .NET search interface includes non-SharePoint content, also verify that you have access to this content.

**4.14.4 Configuring the Claims-Aware Coveo Search Application**

This topic describes how to set up a Coveo search application to allow a seamless experience for Coveo end-users searching for secured content indexed from Claims-Enabled SharePoint web applications. A Claims-aware Coveo search application allows Claims-authenticated users to not have to log in to the Coveo .NET search interface outside of SharePoint to see search results matching their Claims.

**Note:** A better SSO solution that works with or without ADFS is now available (see "Manually Configuring a .NET Search Interface Claims SSO for an On-Premises SharePoint" on page 178).
Requirements:

- SharePoint web applications must be using ADFS 2.0 as a Trusted Identity Provider.
- Configuration will be required on the ADFS server used by SharePoint in order for Coveo search users to be authenticated by ADFS.
- The Coveo SharePoint web service must be installed on your SharePoint server (see "Installing the Coveo Web Service, Search Box, and Search Interface into SharePoint" on page 1309).

Limitation:

- Claims-Based SharePoint web applications using Windows authentication (NTLM or Kerberos) will still require users to enter their Windows credentials in the Coveo Search prior to the initial search.

The procedure consists of the following steps:

- "Step 1: Enabling Claims Authentication on the Coveo Search Site" on page 184
- "Step 2: Creating the Coveo Relying Party Trust" on page 186
- "Step 3: Editing Claims Rules for the Coveo Relying Party Trust" on page 186
- "Step 4: Editing Claims Rules for the SharePoint Relying Party Trust" on page 186
- "Step 5: Configuring the Coveo Service Account for ADFS Identity Delegation" on page 187
- "Step 6: Performing the First-Time Setup on the Coveo Search Site" on page 187

4.14.4.1 Step 1: Enabling Claims Authentication on the Coveo Search Site

Enabling Claims authentication on a search site consists mainly in modifying the web.config file of the search website using the FedUtil.exe tool that comes with the Windows Identity Foundation (WIF) SDK.

1. Using an administrator account, login to the Coveo Front-End server.
2. In IIS, add an HTTPS binding to Coveo .NET Front-End web site.
3. Download and install the WIF SDK for Microsoft .NET Framework 3.5 (see Windows Identity Foundation SDK).

   Note: WIF is included in Microsoft .NET Framework 4.5, but currently, Coveo assemblies rely on the Microsoft .NET Framework 3.5.

4. Start FedUtil.exe that is typical in C:\Program Files (x86)\Windows Identity Foundation SDK\v3.5\.

   Note: For the details on the FedUtil.exe tool refer to the Microsoft documentation (see Establishing Trust from an ASP.NET Relying Party Application to an STS using FedUtil).

   a. In the first screen, specify the path to the web.config file (by default: C:\Program Files\Coveo .NET Front-End 12\Web\) and the URL to the search page with a slash at the end (ex.: https://machinename/).
b. In the second screen:

i. Select the Use an existing STS option and then specify the URL of the federation metadata document (ex: https://adfs01.mycompany.com/FederationMetadata/2007-06/FederationMetadata.xml).

ii. Click Test location to validate that the URL is valid.

c. In the third screen, select the option that corresponds to whether certificate chain validation should be enabled or not.

d. In the next screen, select the option that corresponds to whether security tokens should be encrypted or not.

e. In the next screen (claim list), click Next.

f. In the final screen, click Finish.

Note: The important file to configure the trust relationship in ADFS is: [coveo_web_site_folder]\FederationMetadata\2007-06\FederationMetadata.xml

5. In Internet Information Services (IIS) Manager:

a. Ensure that the Windows Authentication is enabled on the search site by clicking the site in the tree view to the left, and then > IIS > Authentication.

You may need to disable all the other authentication methods for Claims authentication to work.

b. For Claims authentication to work, the application pool pipeline mode must be Integrated (not Classic). Ensure that the website is using an application pool that is configured correctly. Either modify the application pool (if only the Coveo search site is using it) or create a new application pool and make the website using it:

i. Click the site in the tree view to the left > Basic Settings.

ii. Click Application Pools almost at the top of the tree view to the left > click on the application pool in the list > Basic Settings.

Important: In IIS, the searchAdmin site under Coveo .NET Front-End 12 corresponds to the .NET search interface and by default shares the CESAppPool Front-End application pool with the Coveo .NET Front-End 12 site (the search page). The application pool pipeline mode must stay to Classic for the searchAdmin site (the .NET search interface) to work, otherwise a user will get the following message when trying to access the .NET search interface:

Server Error in Application "COVEO .NET FRONT-END 12/SEARCHADMIN"
HTTP Error 500.24 - Internal Server Error
An ASP.NET setting has been detected that does not apply in Integrated managed pipeline mode.

The solution is to create another application pool, assign it to the searchAdmin site, and ensure the application pool pipeline mode is set to Classic.

6. Using a text editor:
a. Open the web.config file.

b. Under `<microsoft.identityModel>`, locate the `<service>` tag.

c. Add the "saveBootstrapTokens" attribute as follows:

```xml
<microsoft.identityModel>
  <service saveBootstrapTokens="true">
```

4.14.4.2 Step 2: Creating the Coveo Relying Party Trust

1. Login to the ADFS server which is used as an Identity Provider by SharePoint, hereafter called the Identity Provider ADFS server.

2. Launch AD FS 2.0 Management Console.

3. Select AD FS 2.0 > Trust Relationships.

4. Right-click Relying Party Trusts and then select Add Relying Party Trust.

5. In the new window, select the Import data about the relying party from a file option.

6. Select the FederationMetadata.xml file that was previously obtained in Step 1, and then click Next.

7. Enter a Display Name such as Coveo Claims-Aware Search Site, and then click Next.

8. Select Permit all users to access this relying party, and then click Next.

9. Validate settings on the final page and then click Next to create the new Relying Party Trust.

4.14.4.3 Step 3: Editing Claims Rules for the Coveo Relying Party Trust

1. Select AD FS 2.0 > Trust Relationships.

2. Right-click the Coveo Relying Party Trust and then select Edit Claim Rules.

3. Under Issuance Transform Rules:

   a. Create a new Pass Through or Filter Incoming Claims rule.

      i. Name = Pass through Windows Account

      ii. Incoming Claim Type = Windows Account Name

      iii. Pass through all claims values = true

   b. Click Finish.

4. Under Issuance Authorization Rules, ensure a Permit Access to All Users rule exists, if not create one.

4.14.4.4 Step 4: Editing Claims Rules for the SharePoint Relying Party Trust

1. Select AD FS 2.0 > Trust Relationships.

2. Right-click the SharePoint Relying Party Trust, and then select Edit Claim Rules.

3. Under Issuance Authorization Rules, ensure a Permit Access to All Users rule exists, if not create one.
4. Under **Delegation Authorization Rules**, add a new **Permit Access to All Users** rule or choose to permit a specific user.

5. Under **Issuance Transform Rules**, for each existing rules of the Relying Party Trust and the Claims Provider Trust:
   a. Click **Edit Rule > View Rule Language**.
   b. If the rule language does not contain a check for `Issuer == "AD AUTHORITY"`, skip to the next existing rule, otherwise keep going.
   c. Copy the rule language.
   d. Close the **Edit** window for the current Rule.
   e. Create the new Relying Party Trust rule using the copied rule language:
      i. Click **Add Rule > Send Claims Using a Custom Rule**.
      ii. Paste the rule language and replace **AD AUTHORITY** by **SELF AUTHORITY**.

4.14.4.5 Step 5: Configuring the Coveo Service Account for ADFS Identity Delegation

1. Log on to Coveo Back-End server.

2. Open the Coveo Administration Tool.

3. Select **Configuration > Security > Security Providers**, and then click the Claims for SharePoint On-premises security provider that is used to authenticate to ADFS.

4. In the **User Identity** box, add the identity of any Windows account that can be used to authenticate to ADFS.

   **Note:** This account does not require any special permissions on the ADFS server, it is only used to connect to ADFS when performing delegated authentication.

4.14.4.6 Step 6: Performing the First-Time Setup on the Coveo Search Site

Point your browser to the Coveo search site. If the site has been properly configured for Claims, the browser should now be redirected automatically to the ADFS authentication site, then back to the search site, and then to the first-time setup page.

In the first-time setup page (see "Coveo .NET Front-End First Time Setup" on page 47), ensure to fill the options in the Claims section correctly by selecting the claim type that contains the Windows identity (ex: `http://schemas.microsoft.com/ws/2008/06/identity/claims/windowsaccountname`). Upon completion, the Claims options are saved in the `web.config` file.

Back to the search page, execute a query. In an interface showing results from a Claims-authenticated source such as SharePoint, results should now show up. In the same manner, queries in the **All Content** interface should now include results from the Claims-authenticated source.

4.14.5 Configuring SharePoint Search Scopes

**Coveo .NET Front-End 12.0.960+ (September 2014)**
SharePoint 2016 (Coveo .NET Front-End 12.0.1633+ (September 2016)), 2013, and 2010 allow SharePoint administrators to define search scopes to allow users to choose to limit their searches to certain criteria such as locations or content marked with particular property values (see Microsoft article Define scopes for searches).

A SharePoint site administrator can define SharePoint scopes even with limited access to SharePoint front-end servers. SharePoint scopes are saved directly in the SharePoint database at the site collection level. Along with the scopes themselves, a default scope configuration can be created at the site collection level. SharePoint scopes are sent to the CES index at query time, as query expressions. Because SharePoint scopes exist only in SharePoint, they can only be used from inside SharePoint pages. A Coveo search page not integrated to SharePoint cannot use them.

**Note:** The support for SharePoint scopes is different from the Coveo search scope that are defined on the Coveo Master server and used in Coveo .NET Front-End user interfaces. An administrator managing Coveo search scope must have access to Coveo Administration Tool and the Coveo .NET Front-End Interface Editor.

Functionally speaking, SharePoint scopes behave similarly to Coveo search scopes. In SharePoint, they appear in the scope drop-down list beside the Coveo search box and in the Search In facet in the results page. When a user selects a SharePoint scope, documents are filtered in or out according to the SharePoint scope configuration.

To configure SharePoint Search Scopes

1. Ensure that Coveo .NET Front-End version 12.0.960+ (September 2014 monthly release) is installed on your SharePoint server (see "Installing the Coveo Web Service, Search Box, and Search Interface into SharePoint" on page 1309).

2. Access SharePoint with a site administrator account.

3. In any SharePoint page containing a Coveo search box, click the gear icon next to the search box, and then select one of the following options:

   - **Current site collection’s scopes** to define or modify the default site collection scopes used by default by every site.
Current site's scopes ([SiteName]) to define a scope configuration applicable only to the current site ([SiteName]), overriding the inherited default.

Notes:
- Alternately, in a Coveo .NET Front-End search interface integrated in SharePoint, from the Do more menu, you can select the same options.
- The gear icon and the Do more menu Current site collection's scopes option are not available to non administrator users.

In the Search Scopes (Site Collection Default) or Search Scopes (Current Site) dialog box, you can perform various actions.

To use default scopes for a specific site, select the Use default scopes (site collection) option.

To specify which scopes are available to end-users, in the Name column, select the checkbox in front of the scope(s) names to make available.

To specify the default scope, in the Default column, select the appropriate scope.

To make selected scopes visible to end-users:
Select the **Show scope selector drop-down next to search box** option to make scopes available in SharePoint from a list next to the search box.

**Note:** By default, the following standard scopes are not included in the scope selector drop-down: All SharePoint, Current SharePoint site, Current SharePoint top level site, All Results, and all the search scopes defined in the Administration Tool.

To include these scopes in the scope selector drop-down, you must edit the **SearchBox.ascx** file of the SharePoint skin:

a. With an account that has administrator rights, access the SharePoint server.

b. Open the **SearchBox.ascx** file with a text editor.

   Depending on your SharePoint version, the file is located in `C:\Program Files\Coveo .NET Front-End 12\Web\Coveo\Skins\SharePoint 2010` or in `C:\Program Files\Coveo .NET Front-End 12\Web\Coveo\Skins\SharePoint 2013`.

c. Remove the following method from the file:

   ```
   protected override void OnInit(EventArgs p_Args)
   {
   ISearchBox sb = Parent.Parent as ISearchBox;
   if (sb != null) {
   sb.ShowStandardScopes = false;
   }
   base.OnInit(p_Args);
   }
   ```

d. Save the file.

Select the **Show scope selector facet in search interface** option to make scopes available in the **Search In** facet of a Coveo .NET Front-End search interface integrated in SharePoint.

To create a new scope or edit an existing one:

Click **Create Scope** to create a new scope or click the **Edit Scope** icon to edit an existing one, and then in the **Search Scope Modification** dialog box, configure the scope:
a. In the **Name** box, enter a meaningful name for the scope. End-users will see this name in the lists of available SharePoint scopes.

b. In the **Description** box, optionally enter a description for the scope. This information is only visible to administrators.

c. Click **Add Rule** when you want to add a new rule to the scope.

d. In the **Rules** list, for each rule:

   i. In the first column, select one of the available rule types:

      o **Web Address**

         A web address rule is used to restrict the scope to only search from a specific SharePoint server part.

         **Example:** You enter [https://intranet.mycompany.com/HumanResources/](https://intranet.mycompany.com/HumanResources/) to create a scope restricted to human resources content.

      o **Field**

         A field rule is used to match the documents for which a given field has a specific value. In a field rule, you can only use fields for which the **Include for field queries** option is selected in the Administration Tool. While you type the field name, an auto completion pop up window suggests the available field names matching typed characters.

         **Example:** A scope with the following field rule would return only PDF files.

         ```
         @sysfiletype = pdf
         ```

      o **Free Text**

         The free text rule value is added as-is to the query sent to the index. Only documents containing the entered keywords are returned. If more than one word is specified, only the documents that contain all the words are returned.
The free text rule can be particularly useful to enter more complex queries using various query syntax elements.

**Example:** A scope with the following query, using fields and a Boolean operator, would return only PDF files from the Engineering site.

```plaintext
@sysspsitename="Engineering" AND @sysfiletype="pdf"
```

ii. In the middle column of the list, enter or select appropriate values for the rule type.

iii. In the second-to-last column, select the action determining how each rule combines with others to form the final scope:

   - **Require (AND)**
     Use this action to narrow search results to documents matching the rule criteria.
   - **Include (OR)**
     Use this action to expand search results by adding documents matching the rule criteria.
   - **Exclude (NOT)**
     Use this action to narrow search results by excluding documents matching the rule criteria.

iv. Click the Delete Rule icon to delete a rule from the scope.

   - Click **Save** to save your scope configuration.

   - To delete an existing scope, click the Delete Scope icon for the scope.

   - Click **Apply** to make your search scope changes effective.
5. Migration

This section regroups topics that help you smoothly migrate your index and .NET search interface configurations from Coveo Platform 6 to Coveo Platform 7.

5.1 Coveo Platform 6 to 7 Migration Overview

The Coveo Platform 7.0 comes with numerous new features. With the software installers and import tools of the Coveo Platform 7, you can smoothly migrate your index and .NET search interface configurations.

The format of the CES 7.0 index changed to reduce its footprint, improve performances, and implement several key new features. The index format change implies that you must re-index all your sources with the new CES 7.0 instance.

**Important:** The side-by-side installation of Coveo Platform 6.x and 7.0 instances on the same server (or set of servers like Master and Mirror servers) is not supported.

When your Coveo Platform 6.x implementation includes customized components developed by Coveo Professional Services or by your own personnel, before starting the migration process, contact the Coveo Support or the Coveo Professional Services to determine how to migrate the customized components.

To migrate a Coveo Platform implementation from version 6.x to 7.0

1. Revise your current Coveo server topology (see "Coveo Scalability Model" on page 14, "Planning Repositories to Index" on page 23, and "Planning .NET Search Hubs and Search Interfaces" on page 24).

2. Provision a new set of servers that fulfill the hardware requirements for your selected server topology or ensure that your current Coveo servers have sufficient free resources to run both versions concurrently (see "Coveo Platform Hardware and Software Requirements" on page 3).

   **Example:** You can use new servers for back-end components and consider sharing the front-end servers as the query rate typically transfers from the original instance to the new one.

3. Install CES on your Master server (see "Installing CES on the Master Server" on page 28).

4. Import your Coveo Platform 6.x configuration (see "Creating a New Index or Importing an Existing CES 6 Index Configuration" on page 40).

   This step is important to smoothly import the configuration for all your collections, sources, connectors, user identities, and many other aspects that you configured from the Administration Tool and the Interface Editor so that you do not have to reconfigure everything manually.

5. With CES 7, all sources must use a security provider. When starting the first time, CES 7 automatically revises the imported configuration and creates security providers as needed for all sources.

   When your implementation includes one or more SharePoint sources, for this type of repository, you however need to manually add the crawling user identity to the SharePoint security provider (see "Creating a Security Provider for the SharePoint Legacy Connector" on page 1341).

6. For a topology with multiple back-end servers:
a. When your topology includes one or more Mirror servers, install the Coveo Mirror components (see "Installing CES Mirror Components" on page 57).

**Note:** By default, the remote converter components are installed on a Mirror server.

b. When your topology includes one or more Remote Converter servers, install the Coveo Remote Converter components (see "Installing CES Remote Converter Components" on page 62).

c. When two or more Master/Mirror servers are available, consider setting them up in a network load-balancing configuration (see "Configuring Coveo Servers in a Network Load-Balancing Cluster" on page 98).

7. Install the Front-End components:

**Note:** Starting with the Coveo Platform 7, the front-end components (Coveo .NET Front-End 12) are distributed, installed and versioned separately from the back-end components (Coveo Enterprise Search 7).

a. Install the Coveo .Net Front-End 12 components on all Front-End servers of your selected topology. In the case of a one server topology, simply run the installer on the Master server (see "Installing Coveo .NET Front-End" on page 43).

b. Import the CES 6.5 .NET search interface settings.

In step 4, the customized .NET search interface settings were imported from the CES 6.x index configuration file (\[Index_Path]\config\config.txt) to the same file for the CES 7 instance. With the Coveo .Net Front-End 12 however, the customized .NET search interface settings are no longer stored in the index configuration file but rather in XML files located in the [.NET_Front-End_Path]\Web\Coveo\Skins folder. You can easily perform this configuration transfer from the Interface Editor (see "Importing CES 6.x .NET Search Interface Settings" on page 643).

c. In the case of multiple Front-End servers, use the Interface Editor deployment tool to replicate the .NET search interface configurations to all servers (see "Deploying Search Interface Settings" on page 647).

**Note:** With the Coveo Platform 6.x, the .NET search interface settings were stored centrally in the index configuration file. Changes were automatically applied to all Coveo Front-End servers but this scheme did not allow to easily set up a staging Front-End server. With the Coveo .NET Front-End 12, the search interface settings are rather saved in XML files on each Coveo Front-End server, allowing you to develop and test settings on one server, and then easily replicate them to one or more production Front-End servers.

d. When your topology includes two or more Front-End servers, consider setting them up in a network load-balancing configuration (see "Configuring Coveo Servers in a Network Load-Balancing Cluster" on page 98).

e. Update the Coveo integration with repositories:
SharePoint

When you integrated Coveo with your SharePoint farm, you must update the Coveo files on your SharePoint servers (see "Installing the Coveo Web Service, Search Box, and Search Interface into SharePoint" on page 1309).

Sitecore

When you integrated Coveo with your Sitecore server, you must update the Coveo web service and the .NET search interface on your Sitecore server (see Installing the Coveo Legacy Web Service Plugin for Sitecore topic in PDF and "Installing Coveo .NET Front-End" on page 43).

5.2 Configuring a Coveo .NET Front-End 12 Server to Use a CES 6.5 Back-End Server

The Coveo .NET Front-End version 12 that comes with the Coveo Platform 7 can also communicate with Coveo Enterprise Search (CES) 6.5 Back-End servers. This compatibility allows you to progressively migrate to the Coveo Platform 7 by starting to use the new .NET search interfaces with your existing CES 6.5 index.

Note: In a geographically distributed index (GDI) configuration, a Coveo .NET Front-End search interface can connect to multiple Back-End servers only when they are of the same major CES version, such as all CES 6.5, or all CES 7.0.

The main tasks to perform are:

- If not already done, install the Coveo .NET Front-End components on a server of your choice (see "Installing Coveo .NET Front-End" on page 43).

- Edit the Coveo .NET Front-End web.config file to instruct the search interface to communicate with a CES 6.5 Back-End Server (see "Configuring the Front-End to Use a CES 6.5 Back-End" on page 195).

- When you install the Coveo .NET Front-End 12 components on a server where the CES 6.5 Front-End components are installed, you must edit three web.config files to be able to use the .NET Interface Editor (see "Editing web.config Files to Enable the Use of the .NET Interface Editor" on page 196).

5.2.1 Configuring the Front-End to Use a CES 6.5 Back-End

1. Using an administrator account, connect to the Front-End server where you installed the Coveo .NET Front-End components.

2. Using a text editor:
   a. Open the \[.NET_Front-End_Path]\Web\web.config file.

   Example: By default, this file is in the C:\Program Files\Coveo .NET Front-End 12\Web\ folder.
b. In the `<coveoEnterpriseSearch>` section, edit the `<server hostname="localhost" port="52800"/>` line:

i. When the CES 6.5 Master server is installed on another server, replace localhost by the name of the CES 6.5 Master server.

ii. When the CES 6.5 Master server uses a CES service port other than the default port, change the `port=` value accordingly (see "About the CES Service Port" on page 230).

**Tip:** You can look in the `web.config` file on your Coveo Platform 6.5 Front-End server that you are replacing to find the `hostname` and `port` values to use.

iii. Add the `enable65SearchAPI="true"` case-sensitive attribute to activate the CES 6.5 compatibility mode.

**Example:** The line is as follows when the server name is `MyCES65Server` and uses the default CES service port: `<server hostname="MyCES65Server" port="52800" enable65SearchAPI="true"/>`

**Note:** When Coveo .NET Front-End 12 is installed on a server different from the CES 6.5 Master server, you must also add the `impersonate="true"` attribute to the `<server hostname="localhost" port="52800" enable65SearchAPI="true"/>` line, and on the CES 6.5 Master server, using the CES 6.5 Administration Tool, you must grant the impersonator permission to the user that runs the AppPool of the Coveo .NET Front-End 12 web application (see Granting Impersonator Privileges).

c. Save the file.

3. Using a browser, open the Coveo .NET Front-End search interface and perform searches to validate that it returns search results from the CES 6.5 Master server.

5.2.2 Editing web.config Files to Enable the Use of the .NET Interface Editor

**Important:** You must perform the following procedure only when you install the Coveo .NET Front-End 12 components on a server where the CES 6.5 Front-End components are also installed. The .NET Interface Editor is working out-of-the-box otherwise.

1. To modify the first `web.config` file:

   a. Using an administrator account, connect to the Front-End server where you installed the Coveo .NET Front-End 12 components.

   b. Using a text editor:

      i. Open the ` [.NET_Front-End_Path]\Web\web.config` file.

      **Example:** By default, this file is in the ` C:\Program Files\Coveo .NET Front-End 12\Web` folder.

      ii. Above the `</coveoEnterpriseSearch>` line, add the following line:

where:

- You edit the coveoPath= value when Coveo .NET Front-End is not installed in the default folder.
- You replace MyCES65Server by the name of your server, or localhost when the Front-End and Back-End components are on the same server.
- You replace 8080 by the appropriate port when your Coveo .NET Front-End server uses a port other than the default.

iii. Save the file.

2. To modify the second web.config file:

   a. Using an administrator account, connect to the CES 6.5 Master server.

   b. Using a text editor:

      i. Open the Microsoft .NET Framework 2.0 web.config file.

      Example: By default, the web.config file folder is:

      - For a 64-bit system: C:\Windows\Microsoft.NET\Framework64\v2.0.xxxxx\CONFIG
      - For a 32-bit system: C:\Windows\Microsoft.NET\Framework\v2.0.xxxxx\CONFIG

      ii. In the <sectionGroup name="coveoEnterpriseSearch"> section, locate and replace the following two lines:

      

      <section name="additionalEditInterfacePages" type="Coveo.CES.Web.Search.Admin.AdditionalPagesConfigSection, Coveo.CES.Web.Search.SearchAdminSite, Version=6.0.0.0, Culture=neutral, PublicKeyToken=44110d16825221f2"/>
      <section name="taggersDefinition" type="Coveo.CES.Web.Search.Tagging.TaggersConfigSection, Coveo.CES.Web.Search, Version=6.0.0.0, Culture=neutral, PublicKeyToken=44110d16825221f2"></sectionGroup>

      by the following two lines:

      

      <section name="additionalEditInterfacePages" type="System.Configuration.SingleTagSectionHandler, System, Version=1.0.3300.0, Culture=neutral, PublicKeyToken=b77a5c561934e089"/>
      <section name="taggersDefinition" type="System.Configuration.SingleTagSectionHandler, System, Version=1.0.3300.0, Culture=neutral, PublicKeyToken=b77a5c561934e089"></sectionGroup>

      iii. Save the file.

3. To modify the third web.config file, still on the CES 6.5 Master server, using a text editor:
a. Open the [CES_Path]\Web\web.config file.

Example: By default, this file is in the C:\Program Files\Coveo Enterprise Search 6\Web\folder.

b. Above the </coveoEnterpriseSearch> line, add the following line:

```xml
```

where:

- You edit the coveoPath= value when CES 6 is not installed in the default folder.
- You replace MyCES65Server by the name of your server, or localhost when the Front-End and Back-End components are on the same server.
- You replace 8080 by the appropriate port when your Coveo .NET Front-End server uses a port other than the default.

Example: The complete section looks like:

```xml
<coveoEnterpriseSearch>
  <server hostname="localhost" impersonate="false" mirrorName="default" port="52800"/>
  <database enabled="false" connectionString="mongodb://localhost/databaseName"/>
  <analytics enabled="false" connectionString="Data Source=yourServerName;Initial Catalog=CoveoAnalytics;Integrated Security=SSPI;"/>
</coveoEnterpriseSearch>
```

c. Save the file.

4. To validate that you can open the .NET Interface Editor, using a browser:

   a. Open the Coveo .NET Front-End search interface.
   
   b. On the Do more menu, select Edit this Interface to access the .NET Interface Editor.
6. CES Moving Scenarios

In the life cycle of your Coveo implementation, you may encounter situations where you need to relocate Coveo Enterprise Search components. This topic provides procedures describing the main steps for a few relocation scenarios.

**Important:** When your Coveo implementation includes Mirror servers, contact Coveo Support for assistance before attempting to relocate CES components.

**Moving CES to another hard disk drive on the same server**

**Example:** The CES installation folder is presently C:\Program Files\Coveo Enterprise Search 7 and you want to move it to D:\Program Files\Coveo Enterprise Search 7 to respect your internal IT rules.

1. From the original hard disk drive, make a backup of all the CES files that you have customized or added (see "About Coveo Platform Folders and Key Files" on page 83).
   - [.NET_Front-End_Path]\Web\Web.config file
   - [.NET_Front-End_Path]\Web\*.aspx added or customized ASP.NET Web pages
   - [.NET_Front-End_Path]\Web\Coveo\Skins added or customized skin folders (see "Moving Skins" on page 204)
   - [.NET_Front-End_Path]\Web\Coveo\bin\*.dll added or customized controls
   - [.NET_Front-End_Path]\Web\Strings\*.xml customized localized user interface strings

2. Uninstall CES (see "Modifying, Repairing, or Uninstalling CES Components" on page 70) because you cannot have two instances of the same version of CES on one server.

3. Reinstall CES, ensuring to click Custom in the Select Setup Type screen to be able to specify installing CES on the new hard disk drive (see "Installing CES on the Master Server" on page 28).

4. Copy all the CES files that you have customized from the backup, and paste them at the appropriate locations in the new CES folders.

5. If you also need to move the index from one hard disk drive to another, use one of the following methods:
   - Relocate the CES configuration folder and rebuild the index on the new hard disk drive (see "Moving the CES Configuration Folder" on page 200).
     This method implies copying a small amount of data but requires to fully crawl and re-index all repositories.
     **OR**
   - Relocate the complete index folder (see "Moving the Index to a Different Hard Disk Drive" on page 202).
     This method implies copying all index files but prevents having to crawl and re-index all repositories.
Moving CES to another server

Example: You started using Coveo on a server meeting the minimum requirements but as more users discover and adopt the Coveo solution, your server no longer has sufficient resources to respond to the demand. You install a more powerful server and want to move CES to this new server.

1. Using an administrator account, connect to the new server.
2. Install CES (see "Installing CES on the Master Server" on page 28).
3. Stop the CES service (see "Stopping the CES Service" on page 251).
4. Migrate the index from the original server to the new server using one of the following methods:
   - Relocate the CES configuration folder and rebuild the index on the new server (see "Moving the CES Configuration Folder" on page 200).
     
     This method implies copying a small amount of data but requires to fully crawl and re-index all repositories.

     OR

   - Relocate the complete index folder (see "Moving the Index to Another Server" on page 203).
     
     This method implies copying all index files but prevents having to crawl and re-index all repositories.

5. On the original server, copy the CES files that you have customized or added (see "About Coveo Platform Folders and Key Files" on page 83).
   - [.NET_Front-End_Path]\Web\Web.config file
   - [.NET_Front-End_Path]\Web\*.aspx files
   - [.NET_Front-End_Path]\Web\Coveo\Skins folder (see "Moving Skins" on page 204)

6. On the new server, paste the CES files at the appropriate locations in the new CES folders.
7. Restart the CES service (see "Starting the CES Service" on page 248).

6.1 Moving the CES Configuration Folder

The Coveo Enterprise Search (CES) configuration folder ([Index_Path]\Config) is automatically created by the CES installer under the index folder that you specify at the end of the installation process (C:\CES7\Config by default).

Important: When your Coveo implementation includes Mirror servers, contact Coveo Support for assistance before attempting to move the configuration folder.

You must relocate the configuration folder when:
You relocate the Coveo index to another hard disk drive on the same server.

*Example:* As your index increases in size, you eventually reach the limit of the hard disk size (see "Coveo Platform Hardware and Software Requirements" on page 3). You then need to add a new larger hard disk and move the index and associated files to the new hard disk drive.

You relocate the Coveo index to another server.

*Example:* As the index size and the number of users increase, the performance of the original Coveo server degrades. You need to replace the server by a more powerful machine and move the index and associated files to the new server.

**Important:** After moving the CES configuration folder, you must rebuild all your sources from all your collections.

To move the CES configuration folder to another hard disk drive on the same server

1. Using an administrator account, connect to the Coveo server on which you want to move the CES configuration folder.
2. Ensure that the new hard disk drive is installed and ready to use.
3. If not already done, create the desired index folder on the new hard disk drive.
   
   *Example:* If D: is the new hard disk drive, you can create the D:\CES7 folder.

4. Stop the CES service (see "Stopping the CES Service" on page 251).
5. Open the original index folder (ex.: C:\CES7), and then copy the Config subfolder.
6. On the new hard disk drive:
   a. Paste the Config subfolder in the new index folder (ex.: D:\CES7).
   b. Open the Config subfolder.
   c. Delete the config.bin file.

   **Note:** CES will automatically recreate this binary version of the configuration file.

7. Change references to the index folder:
   a. In the CES configuration file (see "Changing the Index Folder in the CES Configuration File" on page 205).
   b. In the Registry Editor (see "Changing the Coveo Index Path in the Registry Editor" on page 77).
8. Restart the CES service (see "Starting the CES Service" on page 248).
9. Access the Administration Tool (see "Opening the Administration Tool" on page 256).
10. Rebuild all your sources for all your collections (see "Applying an Action to a Collection or a Source" on page 283).
To move the CES configuration folder to another server

1. Using an administrator account, connect to the new Coveo server, the one to which you want to move the CES configuration folder, and then:
   a. If not already done, install CES, specifying the desired index folder path at the end of the installation process (see "Installing CES on the Master Server" on page 28).
   b. Stop the CES service (see "Stopping the CES Service" on page 251).

2. Using an administrator account, connect to the Coveo server from which you want to move the CES configuration folder, and then:
   a. Stop the CES service (see "Stopping the CES Service" on page 251).
   b. Open the original index folder (ex.: C:\CES7), and copy the Config subfolder.

3. On the new server:
   a. Paste the Config subfolder in the new index folder.
   b. Open the Config subfolder.
   c. Delete the config.bin file.

   **Note:** CES will automatically recreate this binary version of the configuration file.

4. If the index folder paths are not the same on both servers, still on the new server, change references to the index folder:
   a. In the CES configuration file (see "Changing the Index Folder in the CES Configuration File" on page 205).
   b. In the Registry Editor (see "Changing the Coveo Index Path in the Registry Editor" on page 77).

5. Restart the CES service (see "Starting the CES Service" on page 248).

6. Access the Administration Tool (see "Opening the Administration Tool" on page 256).

7. Rebuild all your sources for all your collections (see "Applying an Action to a Collection or a Source" on page 283).

### 6.2 Moving the Index to a Different Hard Disk Drive

You may need to relocate the index to a different hard disk drive on the same server.

**Example:** As your index increases in size, you eventually reach the limit of the hard disk size (see "Coveo Platform Hardware and Software Requirements" on page 3). You then need to add a new larger hard disk and move the index and associated files to the new hard disk drive.

**Important:** When your Coveo implementation includes Mirror servers, contact Coveo Support for assistance before attempting to relocate the index.
To move the index to another hard disk drive

1. Using an administrator account, connect to the Coveo server.
2. Ensure that the new hard disk drive is installed and ready to use.
3. Put the index in read-only mode (see "Toggling the Index Between the Read-Write and Read-Only Modes" on page 263).
4. Stop the CES service (see "Stopping the CES Service" on page 251).
5. Copy the content of the original index folder.
   
   **Note:** The default index folder is C:\CES7 but another folder may have been specified when CES was installed.

6. On the new hard disk drive:
   a. Paste the content of the index folder in the desired folder.
   
   **Example:** When you move the file from the C: to the D: hard disk drives, you can paste the content of the original index folder in the D:\CES7\ folder.
   b. Open the Config subfolder.
   c. Delete the config.bin file.
   
   **Note:** CES will automatically recreate this binary version of the configuration file.
   d. When a [CES_Path]\CES7\Temp folder exists, ensure to delete its content.

7. Change references to the index folder:
   a. In the CES configuration file (see "Changing the Index Folder in the CES Configuration File" on page 205).
   b. In the Registry Editor (see "Changing the Coveo Index Path in the Registry Editor" on page 77).

8. Restart the CES service (see "Starting the CES Service" on page 248).
9. Put the index in read-write mode (see "Toggling the Index Between the Read-Write and Read-Only Modes" on page 263).

### 6.3 Moving the Index to Another Server

You may need to relocate the index to a different server.

**Example:** As the index size and the number of users increase, the performance of the original Coveo server degrades. You need to replace the server by a more powerful machine and move the index and associated files to the new server.

**Important:** When your Coveo implementation includes Mirror servers, contact Coveo Support for assistance before attempting to relocate the index.
To move the index to another servers

1. On the target server, install the same CES version and build that is currently installed on the original server (see "Identifying the Coveo Enterprise Search Version" on page 252 and "Installing CES on the Master Server" on page 28).

2. At the end of the installation process:
   a. When the Create Index page of the Administration Tool appears, under File Locations, in the Folder box, ensure to specify the drive and folder where you want the index to reside on the target server (C:\CES7 by default).
   b. When the Enter License Code page appears:
      i. On the original server, using a text editor, copy the content of the [CES_Path]\Instance\License.txt file.
      ii. Back on the target server, paste the content of the file in the License box.
      iii. Click Apply changes.

3. On the original server, put the index in read-only mode (see "Toggling the Index Between the Read-Write and Read-Only Modes" on page 263).

4. On both the original and target servers, stop the CES service (see "Stopping the CES Service" on page 251).

5. On the target server, open the index folder, and then delete the content of the folder.

6. On the original server, copy the content of the index folder.

7. Back on the target server:
   a. Paste the copied content in the index folder.
   b. When a [CES_Path]\CES7\Temp folder exists, ensure to delete its content.
   c. When the index folder paths are not the same on both servers, change references to the index folder:
      i. In the CES configuration file (see "Changing the Index Folder in the CES Configuration File" on page 205).
      ii. In the Registry Editor (see "Changing the Coveo Index Path in the Registry Editor" on page 77).
   d. Restart the CES service (see "Starting the CES Service" on page 248).
   e. Put the index in read-write mode (see "Toggling the Index Between the Read-Write and Read-Only Modes" on page 263).
   f. In the Administration Tool (see "Opening the Administration Tool" on page 256), in the Index > Sources and Collections page, verify that all your collections and sources are available as they were in the other server.

6.4 Moving Skins

You may need to move the skins from one hard disk drive or one Coveo server to another.
Example: After installing CES on a new Coveo server, you want to move new and customized skins from the original Coveo server to this new Coveo server.

To move all the skins from one hard disk drive or server to another

1. On the target hard disk drive or server where CES is installed:
   a. Open the [.NET_Front-End_Path]\Web\Coveo folder.
   b. As a precaution to be able to revert back to the out-of-the-box skins, make a backup of the Skins folder.

   Example: Copy the C:\Program Files\Coveo .NET Front-End 12\Web\Coveo\skins folder, and then paste it and rename it as C:\Program Files\Coveo .NET Front-End 12\Web\Coveo\Skins_Backup.

2. On the original hard disk drive or server, copy the Skins folder from [.NET_Front-End_Path]\Web\Coveo.

3. On the target hard disk drive or server, paste the Skins folder in the [.NET_Front-End_Path]\Web\Coveo folder.

4. On the target server, reset IIS (see "Resetting IIS" on page 87).

6.5 Changing the Index Folder in the CES Configuration File

When you manually move the CES configuration folder or the Coveo index, you may need to change the references to the index folder in the CES configuration file.

Contact Coveo Support for instructions on how to change the index folder in the CES configuration file.

6.6 About the Index Backup Feature

CES 7.0.6830+ (July 2014)

Coveo Enterprise Search (CES) offers an index backup feature to allow you to safely and efficiently backup your index. During a backup operation, the CES service is maintained so end-users can continue to send queries and receive search results.

The backup feature ensures that the necessary conditions are met to backup and restore a Coveo index:

- Cyclical Redundancy Check (CRC) error-detection is used to validate the backup integrity.
- The index is automatically switched in read-only mode during the backup operation and switched back to the read-write mode after the backup is completed, if it was in this mode when the backup operation was launched.
- System schedules are not allowed to switch the index to the read-write mode during a backup operation.
Notes:

- You can also back up only your configuration files (see "Backing Up and Restoring the CES Configuration Files" on page 216).
- **CES 7.0.7022+ (September 2014)** You can back up and restore:
  - An index containing more than one slice (see "About Index Slices" on page 18).
  - An index for which Near Real-Time indexing is enabled (see "About Near Real-Time Indexing" on page 350).
  - An index for which the configuration file is not saved at the same location as the index files.
- When you run CES in a virtual environment, you can also consider creating snapshots of the virtual machine (VM) on which CES runs to back up the index and the complete CES installation. Before creating a VM snapshot, you must however ensure that the index is switched to the read-only mode (see "Toggling the Index Between the Read-Write and Read-Only Modes" on page 263).
- **CES 7.0.6767– (June 2014)** The creation of a Coveo index backup involves more steps (see "Manually Backing Up and Restoring the Index" on page 215).

### 6.6.1 Backing Up the Index From the Administration Tool

A **System Administrator** can use the Index Backup section in the Administration Tool Welcome page to easily create index backups with the CES index backup feature (see "About the Index Backup Feature" on page 205). It is recommended to regularly back up your Coveo index to be able to efficiently restore it in a valid and up-to-date state following disruptive events. Creating index backups is particularly important for indexes with large sources that can take significant time and computer resources to rebuild from scratch.

**Tip:** You can automate backups with a job scheduling tool of your choice using PowerShell scripts (see "Back Up the Index With a PowerShell Script" on page 208).

To back up the index from the Administration Tool

1. On the Coveo server, access the Administration Tool.
2. In the Administration Tool, select Support > Welcome.
3. **CES 7.0.7022+ (September 2014)** In the Welcome page, in the Index Backup section:
Index Backup

It is recommended to create backups during off-peak hours to prevent affecting search performance. Administration Tool pages are not available during a backup.

<table>
<thead>
<tr>
<th>Target Folder</th>
<th>F:Backup</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type</td>
<td>Compressed (recommended) Takes less disk space, but more time.</td>
</tr>
<tr>
<td></td>
<td>Uncompressed Takes more disk space, but less time.</td>
</tr>
</tbody>
</table>

⚠️ Warning: Backing up a large Coveo index may take a significant amount of time.

Start Backup

This section appears only if you have the **System Administrator** role (see "About Administration Roles" on page 406).

a. In the **Target Folder** box, select or enter the existing full path where you want to save the backup. The backup operation creates a subfolder with a time stamped name to host the files of each backup.

**Important:**

- Ensure that the index backup target disk has sufficient free space to store the backup files.

The backed up folder size will be smaller than the original index folder because log and temporary files are not included in the backup. When you chose to create a compressed backup, the target folder (ZIP files and a BackupInfo file) will be even smaller.

**Note:** CES 7.0.6942–(August 2014) The compressed backup is contained in a single ZIP file.

- CES 7.0.6942–(August 2014) The index backup feature does not create the **Target Folder** when it does not exist. A message similar to the following one appears in the CES Console and logs:

  Cannot backup index: class CGLFile::AvailableDiskSpaceQueryException: An error occurred while querying the disk free space for [Target Folder]\CESBackup-CES-mm-dd-yyyy-hh-mm-ss.

b. Next to **Type**, select the desired option (*Compressed (recommended)* or *Uncompressed*).

c. Click **Start Backup**.

**Note:** For large indexes, it is recommended to create backups during off-peak hours to prevent performance issues.
The following Administration Tool page appears.

4. You can monitor the creation of the backup files with Windows Explorer by inspecting the target folder in which a subfolder with a date stamp name is created:

CESBackup-CES-[mm-dd-yyyy-hh-mm-ss]

Note: If you ever need to cancel a backup, currently the only method is to stop and restart the CES service (see "Starting the CES Service" on page 248).

5. CES 7.0.7022+ (September 2014) Back in the Welcome page, information such as the duration of the backup and its size appear above the Target Folder box.

6.6.2 Backing Up the Index With a PowerShell Script

CES 7.0.6830+ (July 2014)

It is recommended to regularly back up your Coveo index to be able to efficiently restore it in a valid and up-to-date state following disruptive events. Creating index backups is particularly important for indexes with large sources that can take significant time and computer resources to rebuild from scratch.

It is recommended to use the Coveo Enterprise Search index (CES) backup feature to regularly back up your Coveo index (see "About the Index Backup Feature" on page 205). The backups exclude Coveo index log and temporary files. You can choose to compress the backed up index files to reduce the disk space requirements. The backup operation can be launched using a PowerShell script allowing you to easily automate the creation of index backups at regular intervals. If you ever need to rollback to a backed up index, the restore operation is performed by running the CES server with the -restore parameter in a command line (see "Restoring an Index Backup" on page 213).
When you have one or more Mirror servers, you must only back up the index on the Master server. If you ever need to restore your master index, the indexes on Mirror servers will be synchronized with the restored master index.

To back up the index with a PowerShell Script

**Note:** CES 7.0.6830-7.0.6942 (July-August 2014) The procedure to back up the index is slightly different (see Procedure Prior to CES 7.0.7022).

1. Using an administrator account, connect to the Coveo Master server.

2. Ensure that the index backup target disk has sufficient free space to store the backup files.

The backed up folder size will be smaller than the original index folder because log and temporary files are not included in the backup. When you chose to create a compressed backup, the target folder (ZIP files and a BackupInfo file) will be even smaller.

**Example:** The target folder with a compressed backup looks like the following:

![Example Folder Structure](image)

3. Using a text editor, create an index backup PowerShell script:

   a. Copy and paste the following PowerShell script in the text file:

   ```powershell
   $admin = New-Object -comobject CESAdmin.Admin.7.0
   $admin.Connect('localhost', 'Default')
   $admin.BackupIndex('D:\Backup', $TRUE)
   ```

   b. When you want to create a compressed backup to minimize disk space requirements:

      i. In the $admin.BackupIndex line:

      Replace 'D:\Backup' by the full path to the target folder.

      **Example:**

      ```powershell
      $admin.BackupIndex('E:\CESIndexBackup\Backup20140930', $TRUE)
      ```
Notes:

- The $TRUE parameter indicates the compression option is active.
- The target folder can be on another machine or a file server as long as the account running the script has the permissions to access the path.

Example:

```powershell
$admin.BackupIndex('\corp.mycompany.com\dfs\IT\Backups\CES\Backup', $TRUE)
```

ii. Ensure that the target folder is empty.

The backup operation aborts when the target folder contains files and the following error message appears in the CES Console:

The backup target folder is not empty. The backup process was cancelled to prevent overwriting an existing backup. Ensure the target folder is empty or specify a new folder to create.

Tip: You can automatically include a date/timestamp in the file name to ensure that you create a new file for each backup. Use the following code to replace the one presented in step 3a.

```powershell
$TimeStampFile = "D:\CESIndexBackup\Backup$(get-date -uformat "%Y-%m-%d_%H-%M-%S")"
$admin = New-Object -comobject CESAdmin.Admin.7.0
$admin.Connect('localhost', 'Default')
$admin.BackupIndex($TimeStampFile, $TRUE)
```

c. When you do not want to compress the backed up files, in the $admin.BackupIndex line:

i. Ensure that the target folder exists.

ii. Replace $TRUE by $FALSE.

Example:

```powershell
$admin.BackupIndex('E:\CESIndexBackup\Backup20140930', $FALSE)
```

Tip: You can automatically include a date/timestamp in the folder name to ensure that you always create a new folder for each backup. Use the following code to replace the one presented in step 3a.

```powershell
$TimeStampFolder = "D:\CESIndexBackup\Backup$(get-date -uformat "%Y-%m-%d_%H-%M-%S")"
$admin = New-Object -comobject CESAdmin.Admin.7.0
$admin.Connect('localhost', 'Default')
$admin.BackupIndex($TimeStampFolder, $FALSE)
```

d. Save the PowerShell script file with the .ps1 extension on the Coveo Master server in a folder of your choice.

4. In a Windows PowerShell window:

a. Ensure you have the permission to run a script by running the following command, and then answering Y.

```powershell
Set-ExecutionPolicy RemoteSigned
```
b. Run your PowerShell script by entering the full path of your script file.

5. Validate that the backup operation performs normally:

a. In the CES Console, validate that the following message appears and that it is not followed by an error message.

   Backup on path [your_backup_path] requested.

b. In the target folder, validate that the index files are being copied.

To back up the index with a PowerShell Script using a CES version prior to 7.0.7022

**CES 7.0.6830-7.0.6942 (July-August 2014)**

1. Using an administrator account, connect to the Coveo Master server.

2. Ensure that the index backup target disk has sufficient free space to store the backup file.

   The backed up file size will be smaller than the original index folder because log and temporary files are not included in the backup. When you chose to create a compressed backup, the target ZIP file will be even smaller.

   **Example:** The compressed backup is contained in a single ZIP file and looks like the following:

   ![Example of backup file structure]

3. Using a text editor, create an index backup PowerShell script:

   a. Copy and paste the following PowerShell script in the text file:

   ```powershell
   $admin = New-Object -comobject CESAdmin.Admin.7.0
   $admin.Connect('localhost', 'Default')
   $admin.BackupIndex('D:\Backup.zip', $TRUE)
   ```

   b. Depending on the type of backup you want to make:

   - When you want to create a compressed backup to minimize disk space requirements:
     i. In the $admin.BackupIndex line:

     Replace 'D:\Backup.zip' by the full path to the target ZIP file.

     **Example:**

     ```powershell
     $admin.BackupIndex('E:\CESIndexBackup\Backup20140930.zip', $TRUE)
     ```
Notes:

- The $TRUE parameter indicates the compression option is active.
- The target ZIP file can also be on another machine as long as the same condition is respected.

**Example:**

```powershell
$admin.BackupIndex('\ corp.mycompany.com\dfs\IT\Backups\CES\Backup.zip', $TRUE)
```

ii. Ensure that the path to the target ZIP file exists.

The backup operation aborts when the target folder does not exist and the following error message appears in the CES Console:

```
Connection closed (class CGLFile::AvailableDiskSpaceQueryException: An error occurred while querying the disk free space for [path to folder]).
```

iii. Ensure that the target ZIP file does not exist.

The backup operation aborts when the target ZIP file exists to prevent overwriting a previous backup.

**Tip:** You can automatically include a date/timestamp in the file name to ensure that you create a new file for each backup. Use the following code to replace the one presented in step 3a.

```powershell
$TimeStampFile = "D:\CESIndexBackup\Backup$(get-date -uformat "%Y-%m-%d_%H-%M-%S").zip"
$admin = New-Object -comobject CESAdmin.Admin.7.0
$admin.Connect('localhost', 'Default')
$admin.BackupIndex($TimeStampFile, $TRUE)
```

- When you do not want to compress the backed up files, in the $admin.BackupIndex line:
  
i. Replace 'D:\Backup.zip' by the index target folder path.

ii. Ensure that the target folder exists.

The backup operation aborts when the target folder does not exist and the following error message appears in the CES Console:

```
Connection closed (class CGLFile::AvailableDiskSpaceQueryException: An error occurred while querying the disk free space for [folder path]).
```

iii. Replace $TRUE by $FALSE.

**Example:**

```powershell
$admin.BackupIndex('E:CESIndexBackup\Backup20140730', $FALSE)
```

c. Save the PowerShell script file with the .ps1 extension on the Coveo Master server in a folder of your choice.

4. In a Windows **PowerShell** window:
a. Ensure you have the permission to run a script by running the following command, and then answering Y.

```bash
Set-ExecutionPolicy RemoteSigned
```

b. Run your PowerShell script by entering the full path of your script file.

5. Validate that the backup operation performs normally:

a. In the CES Console, validate that the following message appears and that it is not followed by an error message.

```
Backup on path [your_backup_path] requested.
```

b. In the Windows PowerShell window, wait for the command to return True, indicating that the backup was successfully completed.

What's Next?

It is a best practice to regularly and frequently backup your index. You can use a scheduling software to automate the backup creation by regularly running a PowerShell script.

6.6.3 Restoring an Index Backup

You can use the Coveo Enterprise Search index (CES) backup feature to regularly back up your Coveo index (see "Backing Up the Index With a PowerShell Script" on page 208). Following an unfortunate event where your index becomes unusable, you can efficiently restore your latest backup to avoid having to rebuild all your sources.

To restore an index backed up with the index backup feature

1. Using an administrator account, connect to the Coveo Master server.

2. Ensure that the hard disk on which the Coveo index resides has sufficient free space to receive the restored backup.

   **Note:** When the corrupted index files are in their original location, they will be overwritten by the restored backup files, thus not requiring more disk space.

   If you renamed the folder of the corrupted index files, the original folders will be recreated with the restored backup files, thus doubling the required disk space.

3. When it is not already the case, stop the CES service (see "Stopping the CES Service" on page 251).

4. In a Command Prompt window:

   a. Change to the Coveo Enterprise Search Bin folder (C:\Program Files\Coveo Enterprise Search 7\Bin by default).

   b. Run the CES service in restore mode with the following command:

```bash
CEService7.exe -restore [path to backup folder]
```
Examples:

- You want to restore a compressed index backup that is in the
  E:\CESIndexBackup\Compressed\CESBackup-CES-09-30-2014-10-47-41 folder. You enter
  the command:
  
  CESService7.exe -restore E:\CESIndexBackup\Compressed\CESBackup-CES-09-30-2014-10-47-41

- You want to restore an uncompressed index backup that is in the
  E:\CESIndexBackup\Uncompressed\CESBackup-CES-09-30-2014-10-47-41 folder. You enter
  the command:
  
  CESService7.exe -restore E:\CESIndexBackup\Uncompressed\CESBackup-CES-09-30-2014-10-47-41

Important: You cannot restore backups made with versions prior to CES 7.0.7022 (September 2014
monthly release) since the BackupInfo file has a different format.

Note: CES 7.0.6942– (August 2014)

CESService7.exe -restore [path to backup ZIP file or folder] -verbose

Examples:

- You want to restore a compressed index backup that is in the
  E:\CESIndexBackup\Backup20140730.zip file. You enter the command:
  
  CESService7.exe -restore E:\CESIndexBackup\Backup20140730.zip -verbose

- You want to restore an uncompressed index backup that is in the
  E:\CESIndexBackup\Backup20140730 folder. You enter the command:
  
  CESService7.exe -restore E:\CESIndexBackup\Backup20140730 -verbose

The -verbose parameter at the end is necessary if you want to be notified when the backup is restored.

The backed up index files are restored to their original location, overwriting files if they are still there.

The following dialog box appears when the restore process is completed.
Important: If the backup restore fails or is interrupted, you will not be able to restart the CES service until you successfully restore an index or delete it and rebuild it.

5. When the restore operation is completed, restart the CES service (see "Starting the CES Service" on page 248).

6.7 Manually Backing Up and Restoring the Index

Notes:
- This procedure describes the fully manual method to backup an index.
- CES 7.0.6830+ (July 2014) It is recommended to use the index backup feature to safely and more efficiently create index backups (see "About the Index Backup Feature" on page 205).

Like other information system, it is a disaster recovery plan best practice to regularly back up your Coveo index to minimize search down time in the case of an unplanned major issue. Backing up your Coveo index is especially important when it includes sources with a large number of documents that can take a significant amount of time and computing resources to rebuild from scratch.

You must back up the index while the index is in read-only mode or when the CES service is stopped. In both cases, the index files are not locked by a CES process so you can integrally copy all index files. It is recommended to use the read-only mode so that end-users can continue to send queries and receive search results during the backup process. When the CES service is stopped, end-users cannot perform queries. When restoring the index, you however must stop the CES service.

Tip: You can use the system schedules to automatically set your index in read-only mode at specific times (see "Modifying System Schedules" on page 439) and synchronize an automated index backup.

Important:
- When your Coveo implementation includes Mirror servers, contact Coveo Support for assistance in backing up and restoring your index.
- It is highly recommended to regularly back up the CES configuration files (see "Backing Up and Restoring the CES Configuration Files" on page 216).

Note: When you run CES in a virtual environment, you can also consider creating snapshots of the virtual machine (VM) on which CES runs to back up the index and the complete CES installation. Before creating a VM snapshot, you must however ensure that the index is switched to the read-only mode (see "Toggling the Index Between the Read-Write and Read-Only Modes" on page 263).

To back up the index

1. Using an administrator account, connect to the Coveo Master server.
2. Put the index in the read-only mode (see "Toggling the Index Between the Read-Write and Read-Only Modes" on page 263).
3. Copy the content of the original [Index_Path] folder (C: \ CES7 \ by default).
Note: In read-only mode, exclude the files in the C:\CES\Temp\ subfolder from the backed up content as the files in this folder are used by the index as a temporary cache for user queries and will be locked by CES. These file are not required to perform an integral index copy.

4. Paste the copied content in a backup location of your choice.

5. When the paste process is completed, put the index back in the read-write mode (see "Toggling the Index Between the Read-Write and Read-Only Modes" on page 263).

To restore the index from a backup copy

1. Using an administrator account, connect to the Coveo Master server.
2. Stop the CES service (see "Stopping the CES Service" on page 251).

   Important: Restoring a backup copy of an index while indexing or while in read-only mode will most likely result in a corrupted index.

3. Delete all files and folders under the [Index_Path] folder (C:\CES\ by default).

   It is mandatory to delete the existing index files. Otherwise, the transactions generated by the current index will remain in the subfolder while the new index files are being copied. Later on, CES will try to apply these transactions and this will most likely result in a corrupted index.

   Note: When you have sufficient disk space on your Coveo Master server to hold two versions of the index, you can simply rename the [Index_Path] folder rather than deleting its content.

4. Restore the index backup files to the [Index_Path] folder.
5. Restart the CES service (see "Starting the CES Service" on page 248).

6.8 Backing Up and Restoring the CES Configuration Files

It is highly recommended to regularly back up the CES configuration files. In the case of a disaster recovery, you can completely rebuild your Coveo index from a restored copy of the CES configuration files.

You must back up CES configuration files while the index is in read-only mode or when the CES service is stopped. In both cases, the CES configuration files are not locked by a CES process so you can integrally copy them. It is recommended to use the read-only mode so that end-users can continue to send queries and receive search results during the backup process. When the CES service is stopped, end-users cannot perform queries. However, you must stop the CES service to restore the CES configuration files.

Tip: You can use the system schedules to automatically set your index in read-only mode at specific times (see "Modifying System Schedules" on page 439) and synchronize an automated backup of CES configuration files.

Important: When your Coveo implementation includes Mirror servers, contact Coveo Support for assistance in backing up and restoring your CES configuration files.
To back up the CES configuration files

1. Using an administrator account, connect to the Coveo Master server.

2. Put the index in read-only mode (see "Toggling the Index Between the Read-Write and Read-Only Modes" on page 263).

3. Copy the content of the \[Index_Path]\Config\ folder (C:\CES7\Config\ by default).

   **Note:** If your sources use preconversion or postconversion scripts files that are not located under the \[Index_Path]\Config\ folder, ensure to back them up as well.

4. Paste the copied content in a backup location of your choice.

5. Put the index back in read-write mode (see "Toggling the Index Between the Read-Write and Read-Only Modes" on page 263).

To restore the CES configuration files from a backup copy

1. Using an administrator account, connect to the Coveo Master server.

2. Stop the CES service (see "Stopping the CES Service" on page 251).

   **Important:** Restoring a backup copy of the CES configuration files while indexing or while in read-only mode will most likely result in a corrupted index.

3. Delete all files and folders under the \[Index_Path\] folder (C:\CES\ by default).

   It is mandatory to delete the existing index files because the index must be entirely rebuilt from the configuration files.

   **Note:** When you have sufficient disk space on your Coveo Master server to hold two versions of the index, you can simply rename the \[Index_Path\] folder rather than deleting its content.

4. Recreate the \[Index_Path]\Config\ folder

5. Restore the CES configuration files backup files to the \[Index_Path]\Config\ folder.

6. Restart the CES service (see "Starting the CES Service" on page 248).

7. Rebuild the sources.
7. Security

Internet search engines such as Google deal with gigantic amounts of publicly available web documents. Within the realm of an organization, enterprise search engines deal with significantly smaller number of documents, but documents come from various repositories and most importantly, they are often secured. An enterprise search engine must carefully manage content permissions to only return search results that the user performing the search is allowed to see in each of the source repository.

Most on-premises or cloud enterprise repositories come with a security model allowing administrators, and sometimes even users, to set access restrictions to content while other content may remain accessible to all members of the repository, or even any anonymous user.

Some enterprise repositories have distinct authentication means so users have distinct accounts on these repositories and must log on separately to these repositories to access their content.

Example: A person accesses a Search Interface to perform a query matching only two documents in the index, Doc1 in Repo1 and Doc2 in Repo2. The person has three distinct accounts: UserA-Repo1, UserA-Repo2, and UserA-AD. In Repo1, only UserA-Repo1 is allowed to see the document. In Repo2, only GroupY is allowed to see the document, but UserA-Repo2 is a member of this group. Finally, the Repo1 source is configured to chain security providers to link Repo1 users to corresponding AD (Active Directory) users. The Repo2 source is not configured to link users of different types.

When the person performing the search is authenticated as UserA-AD, the index returns Doc1 because UserA-Repo1 is allowed to see the document and is linked to UserA-AD in the Security Cache, but not Doc2, even if UserA-Repo2 is a member of GroupY, because there is no link between UserA-AD and UserA-Repo2, so they appear as two different persons.

Several Coveo components are involved to manage permissions, both at indexing and query time. The schema below illustrates the links between the Coveo components in a simple case where two repositories are indexed.
7.1 At Indexing Time

The Coveo components handle permissions at indexing time as follows:

- While crawling a repository, each Coveo **Connector** gets the security entities associated with each indexed documents. Depending on the repository security model, the security entities may be users, groups, profiles, roles, or some other types.

- The **Index** stores the security entities associated with each document. The index is not aware of which users belong to these groups, profiles, etc.

- The **Index** passes the security entities to the **Security Cache** to take care of managing the members of each security entity.

- The **Security Cache** dispatches the new security entities to the appropriate **Security Providers**.

- Each **Security Provider** interrogates the related repository to get the user members for each security entity (user expansion) and returns this information to the **Security Cache**.

- For a given source, **Security Providers** can be chained to link multiple identities. In this case the **Security Cache** refers to each chained security provider to link the different users in each repository corresponding to the same person (user mapping).

- As a result, the **Security Cache** contains all members of all security entities as well as all linked users (see "What Is a Security Cache?" on page 264).

7.2 At Query Time

The Coveo components handle permissions at query time as follows:

- A **Person** authenticated as a user in a given repository accesses a **Search Interface** and performs a query.

- The **Index**:
  
  - Receives the query and the user identity.
  
  - Gets all documents matching the query.

  - Interrogates the **Security Cache** to get all security entities to which this user and linked users belong.
Filters documents matching the query to only return documents matching allowed security entities to which the user belongs.

- Returns the filtered results to the **Search Interface**.

- The **Search Interface** displays the results.

### 7.3 Security Cache Update

The permissions in enterprise repositories are typically constantly adjusted as people join, move, or leave an organization. To maintain the security entities information up-to-date:

- Independently from the indexing, the **Security Cache** is updated at a regular time interval so that it contains all current members of all current security entities as well as all linked users (see "What Is a Security Cache?" on page 264).

- The security cache is updated daily at midnight by default to ensure that any security entity changes made in indexed repositories within the last 24 hours are effective in the security cache and consequently, reflected in search results.

- A Coveo administrator can change the security update schedule time or frequency (see What Should Be the Frequency of System Schedules? and "Modifying System Schedules" on page 439).

- A Coveo administrator can manually launch the refresh of the whole security cache (see "Refreshing Security Caches" on page 266).

- Using the Security Browser of the Administration Tool, a Coveo administrator can select one or more specific users or groups and update the security cache specifically for them (see Using the Security Browser).

### 7.4 Security Control Levels in CES

In Coveo Enterprise Search (CES), controlling access to indexed content is a key issue. In CES, access to content can be controlled by multiple security levels, linked to collections and sources that are unified index organization units, as well as security associated with each document in their original system or repository.

#### Collection-level security

You can assign access rules to each collection defined in the unified index. Only users meeting the collection security rules can access documents indexed within one of the sources of the collection (see "Modifying Collection Permissions" on page 279).

**Example:** You define a *Human Resources* collection, and set security rules so that only Human Resources employees can access this content.

#### Source-level security

By default, all users who have access to the parent collection can access the sources of the collection. You can however override these permissions. A user that is explicitly allowed access to a source can see the source documents in the results (including the results excerpt, summary and Quick View) but still needs the document-level permissions to be able to open the document (see "Modifying Source Security Permissions" on page 297).
Example: Within the Human Resources collection, you define a Salary and benefits source, and set security rules so that only authorized users from the Human Resources employees can view source documents in the results. However, these authorized users will be able to open a source document only if they have document-level permissions to do so.

Document-level security

Each system or repository containing documents assigns security rules to the elements it contains following a specific security model. One of the key features of CES connectors is to know the security model of the system or repository for which it is designed to connect to (see "Security" on page 218).

When CES indexes content from a system or repository, you generally set the connector to crawl the system or repository using an account that has full access, so that it can index all the content. For each document, the connector extracts the content of the document but also, the security rules associated with the document. Consequently, the unified index contains the content and the security for each document.

Example: The access to a document in the Salary and benefits source from the Human Resources collection is restricted to only to the Human Resources Director.

When a user performs a query, the Coveo server searches for documents matching the query, and then verifies for each matching document if the user performing the query has access rights to this document. The following diagram outlines the process that CES uses to determine if a document can be included in the search results for a given user.
7.5 Security Model Types

Each enterprise repository follows a security model to control who can access each item it contains. The security model complexity can range from allowing full anonymous access to requiring the resolution of permissions for several security layers. Repository security models can be classified in three types.

**Direct permissions**

A user must be allowed in a single permission set to be able to view a document.

**Restrictive permissions**

A user must be allowed in many permission sets to be able to view a document.
Example: In an Atlassian Confluence collaborative site, permissions can be specified for three entities:

- Global - Applicable to the whole site
- Space - Applicable to a given Space (a space is a main subdivision in a Confluence site)
- Page - Applicable to a specific document

A user must have read access from all three permission sets to be able to see the document. A user will not be able to see a document when he is denied in any of these permission sets.

Permissions with priority

Two or more security layers are considered sequentially. A user may be unknown in a first security layer (no permissions set for him) in which case the next security layer is referred to. The first layer that specifies permissions for a user is applied. Following priority layers are not considered.

Example: In an NTFS file system, you can set permissions on a folder. The folders and files it contains inherit these permissions (File Share Permissions). You can also set explicit permissions on a file (NTFS Permissions). The explicit permissions have a precedence on the inherited permissions. When they are set, inherited permissions are not considered.

Tip: From the CES Administration Tool, you can see the permission levels and sets and review the associated security entities from the Index Browser (see "Reviewing Document Details from the Index Browser" on page 375).

Note: From one type of repository security model to another, the priority of the Allowed permission over the Denied permission or the priority of User permissions over Group permissions may be reversed.

What's Next?

Understand how CES reproduces the security model for each document in each repository (see "Permission Levels and Sets" on page 223).

7.6 Permission Levels and Sets

Each indexed repository may have a particular security model (see "Security Model Types" on page 222). With CES 6.5 and 7.0, a document in the unified index has two sets of permissions for security entities (like users or groups):

- Allowed security entities
- Denied security entities
Denied permissions take precedence over allowed permissions. The connectors can reproduce the repository security model by resolving for each document the intersection of all permissions sets from all security layers.

New Permission Levels and Sets

Starting with the CES 7.0.5388 April 2013 monthly release, a document in the unified index may be assigned permissions from more than one security layer (called Permission levels), each containing one or more Permission sets. This feature allows to more easily and more transparently reproduce repository security models. The intersection of multiple permission levels and sets is done by a background security cache management process rather than by the connector at indexing time. Refreshing the security cache allows to pick up changes made in repository groups without having to refresh the source.

Permission set

A permission set consists of a set of allowed and a set of denied security entities and can also allow anonymous access. For a security entity to be considered allowed by a permission set, it must be in the allowed set and not be in the denied set. A security entity can also be unknown to a permission set.

Permission level

A permission level consists of one or more permission sets. For a security entity to be considered allowed by a permission level, it must be allowed by all its permission sets and not denied by any permission set. A security entity can also be unknown to a permission level.

Tip: When you use the Index security permissions and specify additional security permissions to index source permission option, these additional permissions become a permission level (see "Modifying Source Security Permissions" on page 297).

Document Permissions

Document permissions is the intersection of one or more permission levels, each containing one or more permission sets.

When a security model uses permissions with priority, for a security entity to be considered allowed, the following algorithm is used to determine the resolved permissions:

- Check the first permission level:
  - If the security entity is allowed or denied, stop and use that permission.
  - If the security entity is unknown, check the next permission level.

- If the security entity is unknown after checking all levels, consider it denied.

Anonymous access

If a permission set allows anonymous access, everyone is considered allowed. Denied entities, however, can still exist and have precedence.
What's Next?

You can see the permission levels and sets for a document and review the associated security entities from the Index Browser (see Reviewing Document Details from the Index Browser).

### 7.7 About the CES Service Logon Account

Coveo Enterprise Search (CES) runs as a software service on the server on which it is installed. All software services require a logon account. Consequently, when you install CES, you must assign a logon account to the CES service.

When your CES server runs on a domain, the CES service logon account must be a domain user that is granted the Active Directory Read Member Of permission because it is used to expand Active Directory groups.

**Note:** If you plan to index file shares with the File connector, the CES service logon account is used by default to crawl the files, in which case the account must also have access to all the files that you want to index. You can however use another account in the connector (see “Setting up a File System Crawling Account” on page 942).

- "Setting or Changing the CES Service Logon Account" on page 225
- "CES Service Logon Account Best Practices" on page 226

### 7.7.1 Setting or Changing the CES Service Logon Account

You originally specify the CES service logon account when you install CES using the following installer screen (see Installing CES on the Master Server).
When CES is already installed, you can change the CES service logon account and password at any time (see "Modifying the CES Log On Account" on page 227).

7.7.2 CES Service Logon Account Best Practices

The best practice is to create a user account dedicated to the CES service with a password that does not change, or does not change frequently. If needed, contact your network administrator to create the account.

The specific user logon account must be a domain account that typically is a local administrator but more specifically needs the following permissions for the CES service to work properly:

- Part of the Users group of the server where CES is installed.
- Part of the Domain Users group of the domain of the server where CES is installed (not required if the server is in a workgroup instead of a domain).
- Read/Write/Execute permissions on the %ProgramFiles% and %ProgramFiles (x86)% folder.
- Full Control on the folder where the index will be stored (default location C:\CES7\).
- Read/Write permissions on the Windows temporary (%TEMP%) folder.
- Will be automatically granted Logon as a Service by the installation program.
Important:

- **CES 7.0.6339– (January 2014)** It is NOT RECOMMENDED to select the Local System account option, because selecting this option can lead to various authentication issues.

- When the password of the CES service logon account changes in Active Directory, you must also manually change the password in the Coveo Enterprise Search 7 Properties to allow the CES service to continue to operate (see “Modifying the CES Log On Account” on page 227).

- When your Coveo Platform implementation uses a topology that includes Coveo Mirror servers, the same logon account must be used on all of those servers.

**Note:** The CES Service logon account does not need to have read access to local, network, or SharePoint files. The best practice is to manage access permissions to content to be indexed at the source level by defining appropriate User Identities when you configure sources for each repository.

### 7.8 Modifying the CES Log On Account

Coveo Enterprise Search runs as a service on the Coveo server. Following the CES installation, you may need to change the CES service logon account or change the password of the account. You need to select an appropriate account with sufficient permissions for the CES service to work properly (see "About the CES Service Logon Account" on page 225).

**Important:** When the password of the CES service logon account changes in Active Directory, you must also manually change the password in the Coveo Enterprise Search 7 Properties to allow the CES service to continue to operate.

**Note:** You can also modify the CES log on account using the Repair option of the CES installer (see "Modifying, Repairing, or Uninstalling CES Components" on page 70), but the procedure described below is simpler.

To modify the CES logon account

1. Using an administrator account, log on to the Coveo server on which you want to change the CES logon account.

2. Open Services (Windows Start menu > Administrative Tools > Services).

3. In the Services window, double-click Coveo Enterprise Search 7.
4. In the Coveo Enterprise Search 7 Properties (Local Computer) dialog box:

**Important:** It is not recommended to select the Local System account option.

a. Select the Log On tab:

b. Select the This account option.

c. Enter the desired valid Active Directory account name in the form domain\username (see "About the CES Service Logon Account" on page 225).

d. Enter the password for the account in both the Password and Confirm password boxes.

e. Click OK.

7.9 Who Has Access to the Administration Tool?

Only a Coveo administrator has access to the Administration Tool. All users members of the local Administrator group on the Coveo Master server are Coveo administrators. The user that runs the CES service is also a Coveo administrator (see "About the CES Service Logon Account" on page 225). The access for to the Administration Tool for these users cannot be disabled.

A Coveo administrator can also grant Administrator privileges to other users. The Coveo Platform 7 features administration roles allowing to grant restricted Coveo administration permissions to various individuals within your organization (see "About Administration Roles" on page 406 and "Assigning Users to Administration Roles" on page 412).
### 7.10 Ports Used By the Coveo Platform

The following table lists all the ports used to access Coveo Platform components or used between Coveo Platform components. Ensure that your network infrastructure allows the traffic between your Coveo instance servers for these ports.

**Note:** The following table does not include the port numbers used by the Coveo Platform connectors to communicate with third-party repositories.

<table>
<thead>
<tr>
<th>Used by</th>
<th>Default port</th>
<th>Purpose</th>
<th>Configuration</th>
</tr>
</thead>
<tbody>
<tr>
<td>Master, Mirror servers</td>
<td>52800</td>
<td>The CES service port, used by Coveo .NET Front-End servers to send queries to Back-End servers.</td>
<td>When installing CES (see &quot;Installing CES on the Master Server&quot; on page 28) or later.</td>
</tr>
<tr>
<td>Master server</td>
<td>52810</td>
<td>Port used by the Coveo Search API to access the new Coveo Search Web Service (see Search SOAP API Home) and the Coveo Admin Web Service.</td>
<td>When creating the index (see &quot;Creating a New Index or Importing an Existing CES 6 Index Configuration&quot; on page 40).</td>
</tr>
<tr>
<td>Master server</td>
<td>8081</td>
<td>Administration Tool access port</td>
<td>When installing CES (see &quot;Installing CES on the Master Server&quot; on page 28).</td>
</tr>
<tr>
<td>Front-End servers</td>
<td>8080</td>
<td>Used to access web .NET search interfaces and the .NET Interface Editor.</td>
<td>When installing the Coveo .NET Front-End (see &quot;Installing Coveo .NET Front-End&quot; on page 43).</td>
</tr>
<tr>
<td>DIP and Desktop Connector</td>
<td>1980</td>
<td>Index content on end-user desktop and laptop computers.</td>
<td>When deploying the Desktop connector and the DIP GPO.</td>
</tr>
<tr>
<td>Coveo Job Scheduling (CJS) service</td>
<td>56000</td>
<td>The Coveo Job Scheduling service uses this port to manage scheduled operations such as runs and jobs executed for the optional Text Analytics module.</td>
<td>When used for the Text Analytics module, can be configured with TAnGO.</td>
</tr>
<tr>
<td>Coveo for Sitecore</td>
<td>5682</td>
<td>When installed on a Sitecore server, Coveo for Sitecore communicates with the CES QueueCrawler using RabbitMQ message queues through port 5682 (not the standard 5672 RabbitMQ port).</td>
<td><strong>CES 7.0.6339+ (January 2014)</strong>, Coveo for Sitecore uses the 5682 port by default (see Installing Coveo for Sitecore).</td>
</tr>
<tr>
<td>Coveo Diagnostic Tool</td>
<td>52580</td>
<td><strong>CES 7.0.6684+ (May 2014)</strong> The Coveo Diagnostic Tool website access port.</td>
<td></td>
</tr>
</tbody>
</table>
### 7.11 About the CES Service Port

The CES service needs an access port for inter-process communications. You can specify the port when you install CES on one or more servers. The default port is 52800.

**Note:** You can also change the CES service port later (see "Changing the CES Service Port" on page 348).

Consider the following guidelines when specifying the CES service port:

- For simplicity, it is recommended to use the default port (52800).
- Validate that the default port (52800) is not reserved for another process on any of the servers where CES will be installed.
- Validate that the default port is respecting the IT regulations within your organization.
- You can use any available port, but when you do not use the default value, you must modify the `web.config` file accordingly on all Front End servers (see "Configuring .NET Front-End Server Query Destination" on page 102).
- In the case of a multi-server Coveo Platform topology:
  - All Back-End Coveo servers must use the same port number.
  - Ensure that the port you selected is open in the firewall or network switches that are present between Coveo servers.
- When two Coveo instances are installed on the same machine, like a CES 6.x and a CES 7.0, each instance must have a dedicated CES service port.

### 7.12 Coveo REST Search API 8.0

The Coveo Platform 7 comes with the Coveo Search API, a REST web service that is used by other Coveo products such as the Coveo JavaScript Search Framework to send queries and receive search results from a Coveo unified index. The Coveo Search API REST endpoint can also be used by custom applications (see REST Search API Home).

As shown in the following diagram, the Coveo Search API acts as a bridge between the front-end search interfaces or applications and a Coveo Enterprise Search (CES) instance maintaining a unified index on the back-end. The Coveo Search API is typically installed on the Coveo Master server, together with CES, but you can install it on any server (see "Installing the Coveo Search API" on page 92).
Once installed, you can configure various aspects of the Coveo Search API such as the index server, certificates, and authentication (see "Customizing and Starting the Coveo Search API" on page 95).

7.13 About the Coveo Search Web Service

The Coveo Platform 7.0 comes with a SOAP Search Web Service that can be used to perform searches from custom search interfaces using Java, Python, .Net, or C++. The Coveo Search Web Service is accessible from the Coveo Master and Mirror servers by default on port 52810. You can configure the service independently for each server (see "Configuring the Search Web Service for a Mirror" on page 354).

You can specify a different port when you create or import the index (see "Creating a New Index or Importing an Existing CES 6 Index Configuration" on page 40). You can also enable/disable and configure the Search Web Service independently for each mirror (see "Configuring the Search Web Service for a Mirror" on page 354).

You can get the list of supported Coveo Search Web Service versions using the following URL form:

https://[CoveoMasterServer]:52810/CoveoSearchService?versions

You can get the Search Web Service function descriptions in a Web Service Description Language (WSDL) form using the following URL:

https://[CoveoMasterServer]:52810/7.0.[n]/CoveoSearchService?wsdl

Example: When your Coveo server hostname is Coveo7 and the Search Web Service version you want to use is 7.0.14, the URL is:

https://Coveo7:52810/7.0.14/CoveoSearchService?wsdl

Note: For more information, refer to our developer documentation:

- Getting Started Using the Coveo Search SOAP API
- Soap Search API - Data Types
- Soap Search API - Methods

7.14 About the Coveo Admin Service

Coveo Enterprise search comes with a SOAP administration service that can be used by other Coveo product (such as Coveo for Sitecore) to perform CES administration tasks on your CES instance.
The Coveo Admin Service is not installed by default when you install CES. You can however use the CES installer to install and set up or change the service security configuration (see Installing CES on the Master Server or Modifying, Repairing, or Uninstalling CES Components). It is highly recommended to secure the Coveo Admin Service. When installed, the Coveo Admin Service runs as a Windows service and is automatically started.

7.14.1 Validating That the Coveo Admin Service Is Running

You can validate that the Coveo Admin Service is running from the Windows Services manager.

You can also validate that the service is accessible (particularly when the service is secured) and at the same time review the WSDL of available functions using the following URL in a browser on your Coveo Master server:

http://localhost/adminservice?wsdl

or, when the Coveo Admin Service is secured (recommended):

https://localhost/adminservice?wsdl

The WSDL is an XML document that looks like the following screen capture.

![WSDL Screen Capture]

**Note:** When the Coveo Admin Service is secured (HTTPS):

- The WSDL page will not be available if no certificate was configured. You must bind a certificate to the port, 443 by default (see Securing the Admin Service - Troubleshooting).

  When you use a self-signed certificate, the browser identifies the certificate as invalid or unsafe, but your browser should offer to accept the risks and see the WSDL.

- When the standard HTTPS port 443 is used by another application on your Coveo Master server, you can change the port (see Securing the Admin Service - Troubleshooting).

7.15 CES and Anti-Virus Software

Coveo Enterprise Search (CES) is very unlikely to be infected or to contribute to spread computer viruses or other malicious programs. Scanning Coveo index files for viruses is possible, but most likely unnecessary.
When the threat mitigation policy of your organization requires that you scan the CES index files for viruses, CES and the anti-virus software operations must be carefully coordinated to prevent important CES issues described below.

### 7.15.1 CES/Virus Considerations

The documents that Coveo connectors download from indexed repositories to the Coveo Master server are saved to .tmp files while they are being indexed. These .tmp files are compressed disk buffers stored in the index temporary folder (typically D:\CES7\Temp), but can also be partly in RAM. Once indexed, the downloaded documents are deleted from the temporary files and/or memory. In the index, the content of downloaded documents is deconstructed only to retain the terms they contain and their position. The cached HTML or Quick View built for non HTML documents are stored in a compressed format.

If a downloaded document was to be infected, the virus signature could not be detected unless the file was decompressed. The downloaded documents are not executed so a virus could not be activated.

With its index two phase commit system, CES constantly creates and deletes temporary and transaction files. An external process such as an anti-virus can block these operations by keeping a lock on scanned files. CES performs a number of retries on locked files to prevent or minimize interferences, but there can still be cases with issues.

Index files are proprietary format binary files, a bit like a database file. They are usually large. They are constantly modified while indexing. Modifications can occur anywhere in the file, not just at the end. An anti-virus software will often require to fully rescan these modified files and interfere with CES processes.

There is a very small probability that a compressed CES file can randomly generate a pattern that matches a virus signature. In such a case, a virus detection would be a false positive.

CES keeps a fair amount of information in various memory caches. An anti-virus memory scan process can run on a Coveo server as long as it does not lock, modify, or delete memory content used by CES.

### 7.15.2 Possible Interferences

The following table presents the possible types of interferences that an virus scan process can have on CES.

<table>
<thead>
<tr>
<th>Anti-virus software operation</th>
<th>Possible impact on CES</th>
<th>Resolution</th>
</tr>
</thead>
<tbody>
<tr>
<td>Scan index files</td>
<td>Reduced performances</td>
<td>None</td>
</tr>
<tr>
<td>Block access for CES to index files</td>
<td>Crash</td>
<td>Restart CES</td>
</tr>
<tr>
<td></td>
<td>Mirror desynchronization</td>
<td>Synchronize mirror</td>
</tr>
<tr>
<td>Modify, delete, or quarantine an index file</td>
<td>Index corruption</td>
<td>Rebuild the entire index</td>
</tr>
</tbody>
</table>

### 7.15.3 Recommendations

In light of the above considerations and possible interferences, our recommendations are:

1. When possible, exclude the [Index_Path] folder (typically D:\CES7) from your virus scan processes.
2. Otherwise, consider the following two alternatives:
7.15.4 Scanning Coveo Files While the Index Is in Read-Only Mode

You can scan most (not all) Coveo index files for viruses when the index is in read-only mode.

1. For each Coveo server, respect the following guidelines to configure your virus scan jobs:
   - Never scan the following Coveo index subfolders for viruses, even when the Coveo index is in read-only mode (CES can still modify their content and the scan process cause interferences):
     - [Index_Path]\Temp
     - [Index_Path]\Log
   - Consider setting up a virus scan job that only and exclusively scans the following Coveo index subfolder while the index will be in read-only mode:
     - [Index_Path]\Config
     - [Index_Path]\Index
     This virus scan job will be shorter, its duration more predictable, and therefore easier to coordinate with index mode changes.
   - Exclude the Coveo index files from all other virus scan jobs.

2. Manually or automatically with a schedule, put the Coveo index in read-only mode (see "Toggling the Index Between the Read-Write and Read-Only Modes" on page 263).

   **Note:** Consider using a CES system schedule to automate the index mode toggling (see "Modifying System Schedules" on page 439).

3. Validate that the Coveo index completed the pending operations and switched to the read-only mode (see "Administration Tool - Details Menu" on page 261).

4. Manually or automatically with a schedule, start the Coveo server virus scan job.

   **Note:** When the Coveo index mode change is scheduled, evaluate the typical time needed by your Coveo index to switch to the read-only mode, and delay the start of the virus scan job accordingly.

5. Validate that the anti-virus scan is completed and inspect the scan results.
Important: If your anti-virus detects Coveo index files that must be modified, moved, or deleted, before performing any of these operations, contact Coveo Support to verify the impact of such interferences with CES and get required recovery steps.

6. Manually or automatically with a schedule, put the Coveo index back in read-write mode (see "Toggling the Index Between the Read-Write and Read-Only Modes" on page 263).

Note: When the Coveo index mode change is scheduled, evaluate the typical time needed to perform the scan, and delay the toggle of the Coveo index back to its read-write mode accordingly.

7.15.5 Scanning Coveo Files While the CES Service Is Stopped

When your Coveo deployment includes load-balanced mirrors, you can turn off the CES service on one mirror to be able to scan all of its Coveo index files while the other mirrors continue to provide search results.

1. Remove the Coveo server that you want to scan for viruses from the load-balanced cluster.

2. On that Coveo server, stop the CES service (see "Stopping the CES Service" on page 251).

3. Perform the virus scan on the Coveo index files.

4. Validate that the anti-virus scan completed and inspect the scan results.

Important: If your anti-virus detects Coveo index files that must be modified, moved, or deleted, before performing any of these operations, contact Coveo Support to verify the impact of such interferences with CES and get required recovery steps.

5. Restart the CES service (see "Starting the CES Service" on page 248).

6. Put the Coveo back in the load-balanced cluster.

7.16 About Search Security Certificate

The Coveo Platform 7 uses an X.509 public key infrastructure (PKI) scheme to secure communications between the Coveo Front-End and Back-End processes. A certificate authority (CA), trusted by all Coveo servers, issues signed search security certificates that are made available to all your Coveo servers. A Coveo Back-End service returns query results to a Front-End server only when it trusts the search security certificate used by the Front-End server.

The use of search security certificates allows the Coveo Front-End and Back-End servers to run on servers with various operating systems and not be dependent on a single security provider like Microsoft Active Directory.

A search security certificate can be defined so that the Back-End server accepts impersonation only from specific trusted users and/or groups and from specific Front-End servers. The Coveo Platform comes with a default search security certificate that specifies no user or server restrictions. You can select or create search security certificates at the end of the Coveo .NET Front-End software installation and later from the search interface Do more menu (see "Coveo .NET Front-End First Time Setup" on page 47).

Each Coveo instance has a search security certificate whitelist that contains the search security certificates that are trusted to perform queries. The whitelist can also specify, for each certificate, the users or groups that can be impersonated to perform queries as well as the trusted machines that can send queries (see "Editing a Certificate Whitelist" on page 240).
7.16.1 Deployed Search Security Configuration

The Coveo Back-End and Front-End installers perform the required configurations to implement the search security certificate. The following elements must all be in place to allow communication between Coveo Front-End and Back-End servers.

Creation and deployment of default trusted CA and certificates

On the Coveo Master server, the files for one default trusted CA, one certificate for the CES Service, one certificate for the local Front-End, and one certificate for the Mirrors are created in the [Index_Path]\Certificates folder.

**Note:** The default search security certificates are created and signed by Coveo.

SSL declaration of the CA and the certificates

On Coveo Master and Mirror servers, an `<SSL>` section in the [Index_Path]\Config\Config.txt file declares the trusted CA file and the default certificates.

**Example:**

```
<SSL>
    <CACertificatePrivateKey>C:/CES7/Config/Certificates/pk-ca.pem</CACertificatePrivateKey>
    <Certificate>C:/CES7/Config/Certificates/cert-ces.pem</Certificate>
    <TrustedCAs>C:/CES7/Config/Certificates/cert-ca.pem</TrustedCAs>
</SSL>
```

The `<TrustedCAs>` element holds the file path to the file holding all the certificate authorities (CA) the mirror trusts. This trusted CA file contains the CAs in the Privacy Enhanced Mail (PEM) format. On a typical install, the trusted CA contains only one CA that signed all the certificates, including the local front-end search security certificate. There is no need to add a trusted CA on typical install because the front-end search security certificate is already trusted.

**Note:** You can however add as many trusted CAs as you wish, by simply appending other CAs to this file.

Addition of the search security certificate to the whitelist

On Coveo Master and Mirror servers, the thumbprint and optional restriction information are added to the `<CertificateWhitelist>` section in the [Index_Path]\Config\Config.txt file, for each search certification that the Coveo instance can trust (see "Editing a Certificate Whitelist" on page 240).

**Example:**

```
<CertificateWhitelist>
    <SearchCertificate ID="28485">
        <Thumbprint>A33AC6887B8B0625656C7ECEC0E3F040AF6DA360</Thumbprint>
    </SearchCertificate>
</CertificateWhitelist>
```

Identification of search security certificate to use for the Admin Web application

On a Coveo Master server, the Admin web application must identify the search security certificate to use in the
<CoveoEnterpriseSearch> section of the [CES_Path]\Web\Admin\web.config file using the
sslCertificatePath attribute.

Example: Identifying the C:\CES7\Config\Certificates\cert-iis.p12 certificate file.

```xml
<CoveoEnterpriseSearch>
  <server hostname="localhost" port="52800" sslCertificatePath="C:\CES7\Config\Certificates\cert-iis.p12"/>
  ...
</CoveoEnterpriseSearch>
```

Identification of search security certificate to use for the Front-End server

On each Coveo Front-End server, each Web application must identify the search security certificate to use in the
<CoveoEnterpriseSearch> section of the [CES_Path]\Web\web.config file using the
sslCertificatePath attribute. The search security certificate file must be available on the Front-End server.

Example: Identifying the C:\CES7\Config\Certificates\cert-iis.p12 certificate file.

```xml
<CoveoEnterpriseSearch>
  <server hostname="localhost" port="52800" sslCertificatePath="C:\CES7\Config\Certificates\cert-iis.p12"/>
  ...
</CoveoEnterpriseSearch>
```

**Important:** With the Coveo Platform 7 Beta 1, the Coveo .Net Front-End installer does not yet include a first
time setup form that allows to easily configure to which Coveo Back-End server the Front-End server connects
and what search security certificate it will use. You must do this configuration manually (see "Manually

7.16.2 Manually Configuring Search Security Certificate

A Coveo server querying another Coveo instance must use a trusted search security certificate to be able to receive
query results from the Coveo Back-End server (see "About Search Security Certificate" on page 235). The search
security certificate file used must be available on both servers. On Front-End servers, the search security certificate
file must be identified in the web.config file of the web application.

**Note:** You can select or create search security certificates at the end of the Coveo .NET Front-End software
installation and later from the search interface Do more menu (see "Coveo .NET Front-End First Time Setup" on
page 47).

The manual search security certificate configuration varies depending on the Coveo instance deployment:

- Front-End and Back-End components on the same server (see "Local Front-End" on page 238).
- Front-End and Back-End components on different servers (see "Remote Front-End" on page 238).
- Front-End querying multiple Back-Ends (see "Remote Front-End querying multiple Coveo instances" on page
  239)
- Back-End querying another Coveo instance (see "Geographically distributed indexing (GDI)" on page 239).
- Coveo search box integrated in SharePoint (see "SharePoint integration" on page 240).
7.16.2.1 Local Front-End

In a simple one server installation, you install the Coveo Front-End components on the same server as the Back-End components. In this case, the file for the default front-end search security certificate is already available on the server (C:\CES7\Config\Certificates\cert-iis.p12 by default).

1. Using an administrator account, connect to the Coveo Master server.

2. Using a text editor:
   a. Open the [.NET_Front-End_Path]\Web\web.config file.
   b. In the <CoveoEnterpriseSearch> section of the file, add the sslCertificatePath="[Search_Certificate_File]" attribute to the <server> element.

   Example: Identifying the C:\CES7\Config\Certificates\cert-iis.p12 certificate file.

   ```xml
   <coveoEnterpriseSearch>
   <server hostname="localhost" port="52800"
   sslCertificatePath="C:\CES7\Config\Certificates\cert-iis.p12"/>
   ...
   </coveoEnterpriseSearch>
   ```

   c. Save the file.

7.16.2.2 Remote Front-End

In a deployment with one or more Coveo Front-End servers and a Back-End server, you must first copy the search security certificate from the Master server to each remote Front-End server.

1. Using an administrator account, connect to the Coveo Master server, and then copy the [Index_Path]\Config\Certificates\cert-iis.p12 file.

2. For each Front-End server:
   a. Using an administrator account, connect to the Coveo Front-End server.
   b. Paste the search security certificate file to a location of your choice.

   Example: You can create a C:\Program Files\Coveo .NET Front-End 12\Web\Certificates\ folder in which to paste the search security certificate file.

   c. Using a text editor:
      i. Open the [.NET_Front-End_Path]\Web\web.config file.
      ii. In the <CoveoEnterpriseSearch> section of the file, add the sslCertificatePath="[Search_Certificate_File]" attribute to the <server> element.
Example: Identifying the certificate file.

```
<coveoEnterpriseSearch>
  <server hostname="localhost" port="52800" sslCertificatePath="C:\Program Files\Coveo .NET Front-End 12\Web\Certificates\cert-iis.p12"/>
  ...
</coveoEnterpriseSearch>
```

iii. Save the file.

### 7.16.2.3 Remote Front-End querying multiple Coveo instances

In a deployment with a Coveo Front-End server sending queries to more than one Coveo instance, the Front-End needs one certificate that is trusted by all the Coveo instances to which it sends queries.

1. Choose one of the CES instances, as the one holding the search security certificate to be used.
2. Using an administrator account, connect to the Master server of the reference Coveo instance, and then copy the certificate file. This will be the search security certificate the Front-End server will be using.
3. Using an administrator account, connect to the Coveo Front-End server.
4. Paste the search security certificate file to a location of your choice.
   
   Example: You can create a folder in which to paste the search security certificate file.

5. For all the other Coveo instances that you want to query:
   a. Using an administrator account, connect to the Master server of the Coveo instance.
   b. In the [IndexPath]\Config\Certificates\cert-ca.pem folder, append the content of the [IndexPath]\Config\Certificates\cert-iis.p12 file found on the reference Coveo instance machine you chose.
   c. Add the search security certificate thumbprint to the certificate whitelist (see "Editing a Certificate Whitelist" on page 240).

### 7.16.2.4 Geographically distributed indexing (GDI)

In a GDI deployment where one Coveo Back-End server sends queries to another Coveo Back-End server, the Coveo instance receiving the query must trust the CA of the querying Coveo instance.

1. Using an administrator account, connect to the Master server of the Coveo instance that sends queries.
2. Using a text editor, open and copy the content of the [IndexPath]\Config\Certificates\cert-ca.pem file.
3. Using an administrator account, connect to the Master server of the Coveo instance that receives the queries.
a. Using a text editor:

i. Open the `[Index_Path]\Config\Certificates\cert-ca.pem` file.

ii. Paste the copied content at the end of the file.

Example: Two trusted CAs in a `cert-ca.pem` file.

```
-----BEGIN CERTIFICATE-----
MIIECjCCAvagAwIBAgIJAlyesp7873moMA0GCSqGSIb3QEBBQUAMIGtMR0wGwYD
VQQKEzRBQDZIByBTZixdOl5mngMga55jLOB7MDkGALUEAxQyzg4NDkwMzIxLTY1
... 
LFJ0m64Bo4yNrv608MCtwKfibPTjQ0ncMAoVZTDFrW37kUF3mRxwE1Bafioay5H
hhd9wXX0jBRHS0zpTUqemHSgYEQ/4/QKQci1VHaAwyX7xQ==
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
AkNBMSAwHgYJKoZIhvcNAQkBFhFzdXBwb3J0QGNvdmVyMVBd
... 
BgkqhkiG9w0BAQUFAAOCAQEApo11dMAxrFkb9/98E2EUeJutoa3LCmbLRhYg3XY
I1tnfLch8SGC10IC2oKErR8jDQqrjVRnt+1F5VVOjlg2fqPMDd0kd721qDF6d
-----END CERTIFICATE-----
```

iii. Save the file.

b. Add the search security certificate thumbprint (for the `cert-iis.p12` and `cert-ces.pem` files) to the certificate whitelist (see "Editing a Certificate Whitelist" on page 240).

7.16.2.5 SharePoint integration

In a deployment where a Coveo search box is integrated with SharePoint, the SharePoint site needs to use the search security certificate of the Coveo instance to which it sends queries.

1. Using an administrator account, connect to the Coveo Master server, and then copy the `[Index_Path]\Config\Certificates\cert-iis.p12` file.

2. Using an administrator account, connect to the SharePoint server.

3. Paste the search security certificate file to a location of your choice.

4. In Internet Information Services (IIS) Manager, right-click on the SharePoint site, and then open the containing folder.

5. Using a text editor:

   a. Open the `web.config` file.

   b. In the `<CoveoEnterpriseSearch>` section of the file, add the `sslCertificatePath="[Search_Certificate_File]"` attribute to the `<server>` element.

   c. Save the file.

7.16.3 Editing a Certificate Whitelist

A whitelist is simply the inverse concept of a blacklist. A certificate whitelist contains all the trusted search security certificates that can be used by a Front-End server to send queries to Coveo Back-End server. Every Coveo
instance has a search security certificate whitelist defined in the [Index_Path]\Config\Config.txt file.

Each search security certificate can include a list of trusted IP addresses from which it can be used as well as a list of trusted identities it can impersonate. By default, both lists are empty, meaning that a certificate can impersonate everyone and can be used on any server.

Certificates are identified by their thumbprint (see "Finding the Thumbprint of a Certificate" on page 241). The thumbprint for a certificate used by a Coveo Front-End server must be added to the whitelist of the Coveo Master server to which it sends queries. The whitelist is automatically populated to all the mirrors of a Coveo instance so there is no need to do this step on the other mirrors if any.

Contact Coveo Support for instructions on how to edit a certificate whitelist.

7.16.4 Finding the Thumbprint of a Certificate

A certificate thumbprint is an hexadecimal string that uniquely identifies a certificate. A thumbprint is calculated from the content of the certificate using a thumbprint algorithm. CES accepts Secure Hash Algorithm 1 (SHA-1) thumbprints in the 40-digit hexadecimal string form without spaces.

Example: When you find the 93 43 67 bf 1c 97 03 3f 87 7d b0 f1 5c b1 b5 86 95 7d 31 33 thumbprint for a search security certificate, you can enter it in a certificate whitelist as follows:

<Thumbprint>934367bf1c97033f877db0f15cb1b586957d313</Thumbprint>

You can find the thumbprint of a certificate using the Microsoft Management Console (MMC), by importing a certificate, and then read its thumbprint in the properties.

Note: You can use other external tools to extract the thumbprint of a certificate. Portecle is one of them with which you can find the thumbprint under the SHA-1 fingerprint section (see http://portecle.sourceforge.net/).

To find the thumbprint of a certificate using the MMC

1. Using an administrator account, connect to the Coveo Master server.
2. Open a Command Prompt window.
3. Type mmc and press the ENTER key.
4. In the Console add a certificate snap-in:
   a. On the File menu, click Add/Remove Snap In.
   b. Click Add.
   c. In the Add or remove Snap-ins dialog box, select Certificates.
   d. Click Add.
   e. In the Certificates snap-in dialog box, select Computer account and click Next.
   f. In the Select Computer dialog box, click OK.
   g. In the Add or remove Snap-ins dialog box, click OK.
5. In the Console certificate snap-in, import the certificate for which you want to view the thumbprint:
a. In the **Console Root** window, expand **Certificates (Local Computer)**.

b. Right-click the **Personal** folder, and then select **All Tasks > Import**.

c. In the first **Certificate Import Wizard** page, click **Next**.

d. In the second **Certificate Import Wizard** page, click **Browse** to locate the file of the certificate for which you want to find the thumbprint, and then click **Next**.

   **Example:** `D:\CES7\Config\Certificates\cert-iis.pem`

e. In the third **Certificate Import Wizard** page, click **Next**.

f. In the fourth **Certificate Import Wizard** page, click **Finish**.

6. In the **Console** certificate snap-in, read the certificate thumbprint:

   a. In the **Console Root** window, expand **Certificates (Local Computer) > Personal > Certificates**.

   b. In the central panel, double-click the certificate that you just added.

   c. In the **Certificate** dialog box:

      i. Select the **Details** tab.

      ii. Select **Thumbprint** in the list and read or copy the thumbprint hexadecimal string.
7. Optionally, on the **File** menu, click **Save** or **Save As** to save the console file for later reuse.

7.17 Sitecore Connector Security Update

A security vulnerability has been identified in our Sitecore Connector plugin for that could allow code to access Sitecore content that would otherwise be inaccessible.

This security vulnerability affects only customers using the following Coveo connectors:

- Coveo for Sitecore
- Sitecore Connector
- Sitecore Legacy Connector

**CES 7.0.6684**—(May 2014) **Coveo for Sitecore 3.0.381**—(April 2014) If you use one of the above connectors, Coveo highly recommends that you upgrade the Coveo plugin on your Sitecore instance to ensure that the vulnerability is fixed for your website.
Note: This security vulnerability does not affect customers using the "Web Pages Connector" on page 13 to index their Sitecore site.

Refer to the following applicable procedure to resolve the vulnerability:

- Security Update for Coveo for Sitecore
  
  Note: In the PDF, search for "Coveo for Sitecore Not Properly Replicating the Sitecore Permission Model".

- Security Update for Sitecore Connector
  OR
  
  Security Update for Sitecore Legacy Connector
  
  Note: In both PDFs, search for “Security Update for Sitecore and Sitecore Legacy Connectors”.

For help installing updates, contact Coveo Support.
8. Coveo Platform On-Premises Products

The Coveo Platform offers a set of on-premises Coveo products and modules designed to operate together to index multiple enterprise repositories and create a unified information access system.

The following diagram presents the high-level architecture of a Coveo on-premises infrastructure that would integrate all available products and modules.

---

**Coveo Enterprise Search**

Invisible to the end users, Coveo Enterprise Search 7 (CES) is the backbone of the Coveo Platform that connects and continuously crawls your siloed enterprise repositories to create a unified index of your enterprise knowledge. CES receives queries from front-end search interfaces, consoles, and dashboards and returns contextually relevant results within one second.

**Coveo JavaScript Search**

Providing search interfaces to end-users, Coveo JavaScript Search is a flexible search interface framework.

---

www.coveo.com
including out-of-the-box search interfaces that can easily be customized and integrated in web environments by an integrator or a developer.

**Coveo Search API**

Coveo JavaScript Search pages communicate with CES through Coveo Search API.

**Coveo for Sitecore**

End users of Sitecore powered websites can get contextual and personalized search results when Coveo for Sitecore is integrated to Sitecore 7.

**Coveo .NET Front-End**

Providing search interfaces to end-users, the Coveo .NET Front-End module offers a set of out-of-the-box full-featured search interfaces. An administrator can use the Interface Editor to customize the interfaces to match the organization needs and branding.

**Desktop Integration Package**

With the Desktop Integration Package, end users can search Coveo unified index content from the Coveo Searchbar floating on the Windows desktop and from the Coveo Sidebar in Microsoft Outlook. They can also index content stored on their local workstation to make it searchable along with other content.

**Usage Analytics Module**

With the optional Usage Analytics module, administrators can set up an on-premises database to record the usage of the Coveo search interfaces. They can then use the Analytics module user interface to review search usage to help optimize and increase adoption of the Coveo information retrieval solution.

**Text Analytics Module**

Administrators can use the optional Text Analytics module to create additional metadata by extracting and indexing themes and named entities from unstructured documents and enable end users to more easily filter and consolidate data from diverse sources.

**OCR Module**

Administrators can use the Optical Character Recognition (OCR) module to extract and index text from images and scanned documents to make them searchable by end users.

### 8.1 Using the CES Console

The **CES Console** shows the activities of the CES service in a window. It displays useful real-time information such as connection, crawling, and indexing operations. The **CES Console** is a helpful tool for monitoring and troubleshooting purposes.
To use the CES Console

1. Access the **CES Console** (Windows **Start** menu > **All Programs** > **Coveo Enterprise Search 7** > **CES Console**).

   By default, the **CES Console** automatically connects to the local default Coveo instance. Activities appear in the window in real-time when CES settings are modified or indexing and querying activities take place.

   **Note:** When you click in the CES Console window, the scrolling pauses. Press the **ESC** key on the keyboard to resume scrolling.

2. You can refine the activities appearing in the window using the parameters available in the **Filter** section.

3. When the CES Console is not connected, click **Connect**. You can also connect to other Coveo servers by clicking **Disconnect** and then **Connect**.
4. In the **Connect** dialog box:
   a. Beside **Connect to**, select the type of Coveo server to which you want to connect. Select **Instance** to monitor the activity of the Master server.

   **Example:** When you run the CES Console on a Mirror server and want to see the activities on this local server, select **Mirror**, and then select **localhost** in the **Server** drop-down list.

   b. In the **Server** drop-down list, select the Coveo server to which you want to connect. Choose **localhost** to see activities of the local Coveo server.

   c. In the **Instance** drop-down list, when more than one Coveo instance is available on the selected server, select the appropriate Coveo instance.

   d. If the instance uses a port other than the default port (52800), select the appropriate value in the **Port** drop-down list (see "About the CES Service Port" on page 230).

   e. Click **OK**.

8.2 Starting the CES Service

Coveo Enterprise Search (CES) runs as a software service on Coveo Back-End servers. By default, the CES Service should be enabled and automatically running when a Coveo Back-End server starts. When for some reason the CES service is not running, you can manually start it.

**Note:** When the CES Service stops unexpectedly, contact the Coveo Support if you need assistance to find out why it stopped and prevent other service interruptions.
To start the CES service using the shortcut

1. Using an administrator account, connect to the Coveo Back-End server on which you want to start the CES service.

2. On the Windows Start menu, select All Programs > Coveo Enterprise Search 7 > Service > Start Service.

To start the CES service from the Windows Administrative Tools

1. Using an administrator account, connect to the Coveo Back-End server on which you want to start the CES service.


3. In the Services window, right-click Coveo Enterprise Search 7, and then select Start in the contextual menu.

4. Verify that Started appears in the Status column for Coveo Enterprise Search 7.

If it is not the case:

- Ensure that the account you used to log on to the Coveo server has administrative rights.
- Verify if the CES service log on account or password has changed (see "Modifying the CES Log On Account" on page 227).

To start the CES service from the command prompt

1. Using an administrator account, connect to the Coveo Master server on which you want to start the CES service.

2. Open a Command Prompt window, and then:
a. Navigate to the [CES_Path]\bin folder (typically C:\Program Files\Coveo Enterprise Search 7\Bin).

b. Type CESService7.exe followed by the desired parameters listed in the Coveo Enterprise Search 7 dialog box, and then press enter.
Example: For test purposes, you may want to run the CES service in standalone mode rather than as a Windows service. To do so enter the following command:

```
CESService7.exe -Standalone
```

The Coveo Enterprise Search 7.0 [Port:52800] [Default] process window appears and shows logs of the CES service activities. Closing this window stops the CES service.

8.3 Stopping the CES Service

Coveo Enterprise Search (CES) runs continuously as a software service on Coveo Back-End servers. You may need to stop the CES service to perform CES maintenance tasks.

**Important:** Stopping the CES service interrupts all Coveo services from the server.

To stop the CES service using the shortcut

1. Using an administrator account, connect to the Coveo Back-End server on which you want to stop the CES service.
2. On the Windows Start menu, select All Programs > Coveo Enterprise Search 7 > Service > Stop Service.

To stop the CES service from the Windows Administrative Tools

1. Using an administrator account, connect to the Coveo Back-End server on which you want to stop the CES service.
3. In the Services window, right-click Coveo Enterprise Search 7, and then select Stop in the contextual menu.
4. Verify that **Started** disappears in the **Status** column for **Coveo Enterprise Search 7**.

### 8.4 Identifying the Coveo Enterprise Search Version

You may want to know which version of Coveo Enterprise Search (CES) is currently installed on servers in your organization.

**Example:** You want to find out if a specific CES feature introduced in a given version is available to you.

**Note:** The Coveo .NET Front-End and Back-End software components are released separately and have independent version numbers (see "About Back-End and Front-End Component Versions" on page 27).

To identify the version of Coveo Enterprise Search on the Back-End

1. On the Coveo server, access the Administration Tool.

2. At the bottom-left corner of any Administration Tool page, read the Coveo Enterprise Search (CES) version information that appears in the following format:

   `[Major].[Minor] [OSBits] Build [Release].[Hotfix]`
8.5 Checking for Available Coveo Enterprise Search Updates

You may want to periodically verify if there are updates available for Coveo Enterprise Search.

**Notes:**

- You can refer to the release notes to get details.
- You can get the latest version of Coveo software products from productupdate.coveo.com.

To check for Coveo Enterprise Search (CES) updates

1. On the Coveo server, access the Administration Tool.
2. On the Administration Tool menu, select **Support**.
3. In the Welcome page, under **Software Update**, click **Check for Coveo Enterprise Search software updates**.
4. In the Coveo Website **Products Updates**, under **Available Updates**, click the download link for the latest available Coveo Enterprise Search 7.x monthly release (32 vs 64-bit version) to download the installer.

   **Note:** Download links for the previous major release may be also proposed under **Other Available Updates**.

5. Run the installer to upgrade CES (see "Upgrading CES" on page 79).

### 8.6 CES Administration Tool

The Coveo administrator uses the Administration Tool to configure all the Coveo Enterprise Search (CES) processes, except for the search interfaces—which are configured through the Interface Editor. The Administration Tool is a web application that runs from each Coveo server (see "Opening the Administration Tool" on page 256).
Note: The user interface of the Administration Tool is available in English and French. When you are in the Administration Tool, you can easily switch from one language to another by pressing the Ctrl+Alt+Page Up keyboard shortcut keys or using an Advanced menu parameter (see "Modifying Advanced CES Parameters" on page 533).

The Administration Tool is organized into eight tabs (see "Navigating in the Administration Tool" on page 257). The following table briefly describes the content of each tab.

<table>
<thead>
<tr>
<th>Tab</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Status</td>
<td>Displays information about past and current CES processes (see &quot;Administration Tool - Status Tab&quot; on page 257).</td>
</tr>
<tr>
<td>Index</td>
<td>Allows Coveo administrator to populate the index with collections and sources, fine-tune ranking, create a thesaurus, configure mirrors and slices, and enable result clustering (see &quot;Administration Tool - Index Tab&quot; on page 269).</td>
</tr>
</tbody>
</table>
### Tab | Description
--- | ---
Content | Displays the content of the index and allows users to test the search function (see "Administration Tool - Content Tab" on page 369).
Reports | Displays charts and statistics concerning the querying process, indexing process, and index content (see "Administration Tool - Reports Tab" on page 386).
Logs | Displays detailed information about the system and the querying and indexing processes (see "Administration Tool - Logs Tab" on page 393).
Configuration | Allows Coveo administrator to configure the CES security parameters, create schedules, manage connectors and converters, describe the structure of documents, enter new license codes, and set system alerts by email (see "Administration Tool - Configuration Tab" on page 405).
Support | Provides links to different support resources.

### 8.6.1 Opening the Administration Tool

You can access the Coveo Administration Tool using different methods.

**Note:** Only a Coveo administrator can access the Administration Tool. As a Coveo administrator, you can grant Coveo administrator permissions to other users with various level or access using administration roles (see "Assigning Users to Administration Roles" on page 412).

To open the Administration Tool

- **Using the Administration Tool URL:**
  1. In a browser address bar, enter the Administration Tool URL in the form:
     
     
     \[\text{[Coveo\_Master\_Server]}:\text{[Port]}\]

     **Note:** Starting with CES 7, the Coveo Administration Tool is directly accessible on a dedicated port from the search interface port. The default Administration Tool port is 8081, but it can be customized.

     **Examples:** When you are logged in to the Coveo server, use: http://localhost:8081
     From any computer, use: http://MyCoveoServer:8081 or

     **Note:** If you get an error when trying to access the Administration Tool from a remote computer, make sure that:
     
     - The URL contains the appropriate port.
     - The firewall on the Coveo server is allowing communications through the port.

     2. In the dialog box that appears, enter your Coveo administrator user name and password, and click **OK**.

- **Using the Windows Start menu:**
1. Using an administrator account, connect to the Coveo Master server.

2. On the Windows Start menu, select All Programs > Coveo Enterprise Search 7 > CES Administration Tool.

Note: CES 7.0.6607 – (March 2014) The page name is Administration Tool.

8.6.2 Navigating in the Administration Tool

The pages of the Administration Tool are organized in a hierarchy starting with a series of tabs at the top of the application followed by an horizontal menu bar. The corresponding content appears below the menu bar.

When a third hierarchical level is necessary, a vertical navigation panel appears on the left side of the page. The corresponding content then appears on the right side of the page.

Note: When a member of an administration role has partial access to the Coveo Administration Tool, the features to which access is restricted (tabs, menus, parameters...) are visible but disabled, appearing shaded.

To navigate to a specific page of the Administration Tool

1. Select the appropriate tab.

2. Select the appropriate menu command.

3. When a third hierarchical level is necessary, select the appropriate item in the navigation panel on the left side of the page.

Note: The Tab > Menu Command > Navigation Panel Item syntax is often used throughout the documentation to quickly identify the location of a page. The > symbol is used as the separator.

Example: In the Administration Tool, go to the Web Connector page (Configuration > Connectors > Web Connector).

8.6.3 Administration Tool - Status Tab
The Status tab contains two menus from which you can see the overall system state and review detailed information on the index content and service status. The features of the Status tab are useful to quickly monitor the state and ongoing activities.

**Overview**

The Overview page displays general information about Coveo Enterprise Search (CES) past and present status. You can use this page to quickly determine which processes are running and which tasks you need to perform (see "Administration Tool - Overview Menu" on page 258).

**Detail**

The Detail page displays information about Coveo Enterprise Search (CES) memory and disk usage. Moreover, it provides links to perform basic maintenance and customization processes (see "Administration Tool - Details Menu" on page 261).

8.6.3.1 Administration Tool - Overview Menu

The Overview page displays general information about Coveo Enterprise Search (CES) past and present status. You can use this page to quickly determine which processes are running and which tasks you need to perform.
<table>
<thead>
<tr>
<th>Section</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Active Sources</td>
<td>Lists the sources currently being refreshed or rebuilt.</td>
</tr>
<tr>
<td>System State</td>
<td>Indicates whether querying and indexing are enabled.</td>
</tr>
<tr>
<td></td>
<td>Click See more to access the Details page (see &quot;Administration Tool - Details Menu&quot; on page 261).</td>
</tr>
<tr>
<td>Index Content</td>
<td>Indicates the number of indexed documents, and between parentheses, their total original size in their repository.</td>
</tr>
<tr>
<td></td>
<td>Indicates the current number of documents to process, convert, or delete (when indexing is being performed), as well as the number of pending transactions.</td>
</tr>
<tr>
<td></td>
<td>Click See more to access the Index Content page.</td>
</tr>
<tr>
<td></td>
<td>Click Commit Current Transaction to force-commit the transaction (see &quot;What Is a Transaction?&quot; on page 259).</td>
</tr>
<tr>
<td>Service Status</td>
<td>Indicates the time (in hours and minutes) elapsed since the CES service was started.</td>
</tr>
<tr>
<td></td>
<td>Click See more to access the Details page (see &quot;Administration Tool - Details Menu&quot; on page 261).</td>
</tr>
<tr>
<td>Disk</td>
<td>Indicates the disk space occupied by CES index.</td>
</tr>
<tr>
<td></td>
<td>Note: Identifiers from deleted documents and terms are automatically recycled by the index self-optimization process (see &quot;About the Index Self-Optimization Process&quot; on page 270).</td>
</tr>
<tr>
<td>Query History</td>
<td>Displays a chart and statistics about the number of queries made in the previous six hours.</td>
</tr>
<tr>
<td></td>
<td>Click See more to access the Query History page (see &quot;What Information Is Displayed in the Query History?&quot; on page 386).</td>
</tr>
<tr>
<td>Index History</td>
<td>Displays a chart and statistics about the documents indexed in the previous six hours.</td>
</tr>
<tr>
<td></td>
<td>Click See more to access the Index History page (see &quot;What Information Is Displayed in the Index History?&quot; on page 386).</td>
</tr>
<tr>
<td>Last Source Refresh/Rebuild</td>
<td>Displays a list of sources recently added, refreshed or rebuilt.</td>
</tr>
<tr>
<td>Recommended Tasks</td>
<td>Displays a list of system tasks to perform. Click a task to access its related page (see &quot;Reviewing CES Recommended Tasks&quot; on page 260).</td>
</tr>
<tr>
<td>License</td>
<td>Displays general license information.</td>
</tr>
<tr>
<td></td>
<td>Click See more to access the License page or Upgrade License to display the Coveo product Web page (see &quot;What Information Is Displayed in the License Page?&quot; on page 525).</td>
</tr>
</tbody>
</table>

8.6.3.1.1 What Is a Transaction?

A transaction is a unit of data that CES keeps in memory until it is written in the index. Instead of constantly writing data, CES waits until its memory cache is filled before committing a transaction. The purpose of this process is to save CPU resources and prevent disk fragmentation by consolidating information. Furthermore, the maximum size of a transaction is limited by the available memory, thus if CES has 50 MB of RAM at its disposal, it commits larger transactions than if it has only 25 MB.
Note: The Coveo administrator can also specify a time limit after which the transaction is automatically written (see "Modifying or Using Advanced Index Parameters" on page 366) or force-commit the transaction (see "Forcing the Commit of a Transaction" on page 260).

Important: End-users cannot query data contained in an unwritten transaction.

8.6.3.1.2 Forcing the Commit of a Transaction

A transaction is a unit of data that CES keeps in memory until it is written in the index. Because the data contained in an unwritten transaction cannot be queried, it can be useful to manually force-commit transactions instead of waiting until they reach their size or time limit, especially when the indexing process is completed.

To force-commit a transaction

1. On the Coveo server, access the Administration Tool.
2. In the Administration Tool, select Status > Overview.
3. In the Overview page, when transactions still need to be written, in the Index Content section, click Commit Current Transaction.

Note: When you often perform this manual operation, consider reducing the time limit after which a transaction is committed (see "Modifying or Using Advanced Index Parameters" on page 366).

8.6.3.1.3 Reviewing CES Recommended Tasks

The CES Administration Tool automatically analyzes your Coveo Enterprise Search (CES) configuration to identify best practice tasks that you should perform to optimize the management of your Coveo deployment and prevent issues.

The following table presents possible recommended tasks.
<table>
<thead>
<tr>
<th>Recommended Task</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Synchronize Mirrors</td>
<td>Synchronize a mirror that is not in the In Sync state.</td>
</tr>
<tr>
<td>Create a Collection of Sources</td>
<td>Build your index starting with at least one collection of one or more sources.</td>
</tr>
<tr>
<td>Setup Mail Alerts</td>
<td>Add mail alerts to be notified of important Coveo Enterprise Search events and issues.</td>
</tr>
<tr>
<td>Setup &quot;Read-Only Mode&quot; Schedule</td>
<td>If you want to automate backups and anti-virus scans of your Coveo index, you must ensure that the index is in read-only mode during these operations. This can be done with schedules.</td>
</tr>
<tr>
<td>Modify the Web Connector User Agent</td>
<td>When you create a Web source, the CES Web crawler identifies itself to the crawled server with the User Agent and User Agent Identifier values. You can modify these values when you want to better identify or track the Coveo crawler on the indexed site, or return specific content for the Coveo crawler.</td>
</tr>
</tbody>
</table>

To review CES recommended tasks

1. On the Coveo server, access the Administration Tool.
2. In the Administration Tool, select Status > Overview.
3. In the Overview page, in the Recommended Tasks section:
   a. Click the task to go to the appropriate Administration Tool page.
   b. When you need more information on the specific task, click Help to access the related online help page.
   c. Perform the recommended task.

8.6.3.2 Administration Tool - Details Menu

The Details page displays information about Coveo Enterprise Search (CES) memory and disk usage. Moreover, it provides links to perform basic maintenance and customization processes. The following table describes each of its sections.
### System State
Indicates whether queries and indexing are enabled and whether the index is in read/write mode or read-only mode.

When queries are disabled, all CPU resources are available for indexing and vice versa. Therefore, disabling queries speeds up indexing and disabling indexing speeds up queries (see "Disabling or Enabling Queries" on page 268 and "Disabling or Enabling Indexing" on page 269). It is recommended to disable indexing while you edit connector parameters.

When the index is in read-only mode, it cannot be modified but queries are enabled (see "Toggling the Index Between the Read-Write and Read-Only Modes" on page 263).

**Note:** It is possible to disable indexing or switch to read-only mode periodically using system schedules (see "Modifying System Schedules" on page 439).

### Content Security
Allows to update the security cache and external security cache (see "Refreshing Security Caches" on page 266).

### Service Uptime
Indicates the time (in hours and minutes) elapsed since the CES Service has started.

### Converter Memory Usage
Displays statistics about the memory use of local and remote converters (see "Administration Tool - Converters Menu" on page 455).

### Mirrors and Slices Resource Usage
Displays statistics about the memory use of mirrors and slices (see "Adding a Mirror Server" on page 338 and "Adding an Index Slice to the Master Server" on page 342).

### Service Resource Usage
Displays statistics about memory and disk use—including the space taken by logs (see "Administration Tool - Logs Tab" on page 393).
8.6.3.2.1 Toggling the Index Between the Read-Write and Read-Only Modes

The normal index mode is the read-write mode in which indexed documents are updated. The index can also be temporarily switched to the read-only mode to process all pending transactions and prevent further modifications to its content, but still enable queries to return results to end-users.

While the index is switching between modes, the Administration Tool pages are unavailable. In the read-only mode, the Administration Tool pages are available but you cannot change index parameter values.

**Important:** The index must be in the read-only mode while:

- You back up, restore, relocate, or scan the index for virus (see "CES and Anti-Virus Software" on page 232).
- If CES runs on a virtual machine, when you create a snapshot of the virtual machine.

The read-only mode ensures that:

- No index files will change during the operation so that the backed up or relocated index is valid.
- The operation does not disturb the index file deleting, renaming, or creation processes involved in the management of transactions so that the index remains and can restart in a valid state.

**Notes:**

- You can switch between read-write and read-only modes automatically following a schedule (see "Modifying System Schedules" on page 439). This is useful to ensure the index switches modes before and after your scheduled backup and virus scan processes (see "CES and Anti-Virus Software" on page 232).

- The index automatically switches to the read-only mode to prevent errors when the index disk free space reaches a minimum of 5 GB, in which case an error message is logged. You can get an email notification when email alerts for fatal errors are configured (see "Configuring Email Alerts" on page 528).

- You can force an index to start in read-only mode by adding the value name `ForceReadOnly` with empty data to the registry key `\HKEY_LOCAL_MACHINE\SOFTWARE\Coveo\Enterprise Search\\\Instance\default`. The `ForceReadOnly` value is automatically deleted when you switch the index to the read-write mode. Forcing a read-only start can be useful for example when troubleshooting an issue where the index repeatedly crashes while in read-write mode. The `ForceReadOnly` feature is available with CES 7.0.6607+ (April 2014 monthly release).

To manually toggle between the read-write and read-only index modes

1. On the Coveo server, access the Administration Tool.
2. Navigate to the Details page (Status > Details).
3. In the System State section, next to the Index is in [current_mode] mode status, click [Switch to Read-Only Mode] or [Switch to Read/Write Mode].
Note: The time required to switch between modes increases with the number of active source crawlers and security providers, particularly when switching from read-write to read-only mode because they must all be stopped before switching.

8.6.3.2.2 What Is a Security Cache?

The Coveo Enterprise Search (CES) security cache maintains lists of relationships between all the security entities (users and groups) for all the indexed repositories. When a user performs a query, CES refers to the security cache to quickly determine the user permissions and therefore return only documents the user is allowed to see. Without the security cache, CES would have to refer to repositories at each query to get the user permissions, leading to very long query response time.

Example: In Active Directory, the mycompany\jsmith account is a member of the qa_team group. This information is stored in the security cache. When the mycompany\jsmith account performs a query, CES refers to the security cache, sees the account is a member of the qa_team group, and includes in search results documents matching the query that are restricted to the qa_team group.

The security cache also stores mappings between accounts in different repositories for each user.

Example: When a mapping between the Windows account mycompany\JSmith and the Lotus Notes account jsmith.mycompany.corp of a user is stored in the security cache, Lotus Notes documents accessible to jsmith.coveo.corp are also returned for mycompany\JSmith.
CES creates and maintains the security cache using the defined security providers to get the security entities and their relationships from the various repositories (see "What Are Security Providers?" on page 417). The security entities and their relationships can change over time in the indexed repositories. Some of these security changes are continuously updated in the security cache.

**Example:** In SharePoint, an administrator creates the Project_A_Team group, assigns users to the group, restricts documents to this group, and refreshes the SharePoint source. Within minutes, a user performs a query for which one or more SharePoint documents restricted to the Project_A_Team group are part of the matching results. CES does not include these documents in the search results, even if the user is a member of the Project_A_Team group, because the group information is not yet available from the security cache.

However, CES identifies that this group is not defined in the security cache and queues a request to get the group members. The group information is added to the security cache as soon as the request is performed, typically within minutes.

A few minutes later, a Project_A_Team group member performs a query for which Project_A_Team restricted documents are matching. They are now included in the search results.

The security cache must however be updated regularly to catch all security changes. By default, the security cache is updated daily at midnight.

**Example:** In Active Directory, and administrator removes the mycompany\jsmith account from the qa_team group. Later that day, mycompany\jsmith performs a query matching qa_team restricted documents that still appear in search results because the security cache has not yet been updated. The next day, mycompany\jsmith performs the same query, but this time, qa_team restricted documents are not included in search results.

**Important:** The security cache does not contain document permission information. The index does. When the permissions on index documents change in a given repository, the change becomes effective in the index following an incremental refresh, a full refresh, or a rebuild of the corresponding source. The type of source action needed to update permission changes depend on the source connector type. Refer to the connector documentation for more information on updating document permissions.

**Note:** CES 7.0.7914+ (October 2015) CES comes with an optimized security cache implementation that can significantly reduce the size of the security cache and the server resources needed to update the cache. New indexes created automatically use the new security cache implementation.

CES 7.0.7814– (August 2015) Index created keep the original cache implementation by default. If it is your case and the update of your security cache takes a significant amount of time and resources, contact Coveo Support to get assistance to enable the new security cache implementation.

8.6.3.2.2.1 External Security Cache

The normal method used by CES to handle document permissions is referred to as *early-binding*, meaning that identifying which users are allowed to access a document is done at indexing time, and stored in the index. With the information maintained in the security cache described above, CES can very quickly return secure search results.
CES can also populate an external security cache for rare cases where it is not possible or not effective to gather permission information at indexing time. In this case, the method used is referred to as late-binding. CES rather determines which documents a user is allowed to see at query time.

When a user performs a query and matching documents are in the late-binding mode, CES checks if the permissions relative to matching documents are in the external security cache. When they are, allowed documents are returned quickly in search results. When they are not, CES uses a security provider to ask the repository if the user is allowed to see each matching document. When the information is returned, CES includes those that are allowed in the search results and adds the collected permission information to the external security cache. Consequently, with this method, the first time a query is performed will be potentially very slow, but next occurrences will be very quick.

**Notes:**

- You can enable late-binding for a source from its Permissions page (see Modifying Source Security Permissions).
- You can reset the external security cache by clicking the Clear External Security Cache Now link from the Details page (see "Refreshing Security Caches" on page 266).

What's Next?

- You can also manually start the security cache update process (see "Refreshing Security Caches" on page 266).
- You can change the security cache update schedule time or frequency (see "Modifying System Schedules" on page 439).
- You can get familiar with how Coveo components deal with permissions on documents both at indexing and query time (see "Security" on page 218).

**8.6.3.2.3 Refreshing Security Caches**

Coveo Enterprise Search (CES) uses a security cache to quickly identify the security identity of a user performing a query. The security cache is updated daily at midnight by default to ensure that any security identity changes made in indexed repositories within the last 24 hours are effective in the security cache and consequently reflected in search results. You can change the security update schedule time or frequency.

As described in the procedure below, you can also manually start the security cache update at anytime to ensure that all the latest permission changes made in all repositories will be effective shortly in search results.
Notes:

- Updating the cache sends requests to all repositories to get all users and groups. When repositories have a large number of users and groups, the repository servers and the Coveo Master server may consume noticeable resources to process the requests. This is why by default, the security cache update is scheduled only once a day during a typical off-peak period.

- When you want to update the security cache for changes made only to one or a few specific security groups, you can efficiently do that using the Security Browser to find each of these groups and then click Update permissions for: [group_name].

- The security cache does not contain document permission information. The index does. When the permissions on index documents change in a given repository, the change becomes effective in the index following an incremental refresh, a full refresh, or a rebuild of the corresponding source. The type of source action needed to update permission changes depend on the source connector type.

- CES 7.0.7183+ (November 2014) The security cache update performance is improved by automatically disabling the update of invalid security entities in the cache. The invalid security entities remain in the security cache to allow to return indexed documents that would still be associated with these entities, but the entity relationships are cleared and these entities will no longer be updated. If invalid security entities return to a valid state, their update in the security cache will automatically be re-enabled.

Example: In the security cache, the group G contains the user U. Document1 allows the group G, and Document2 allows the user U. When the group G or the user U are tagged invalid, the relationship between the group G or the user U is cleared in the security cache. When user U performs the query, only Document2 is returned.

The external security cache rather stores document-level permissions which are not indexed because they are listed in a separate directory.

Example: When mycompany\JSmith queries a repository for which document-level permissions are not indexed, CES has to access the security directory and determine which documents are accessible to mycompany\JSmith. To avoid repeating this lengthy process, CES keeps the permissions granted to mycompany\JSmith in the external security cache for future reference.

You can also manually refresh the security caches between scheduled refreshes.

To manually refresh the security caches

1. On the Coveo server, access the Administration Tool.
2. On the menu, select Status > Details.
3. In the Details page, in the Content Security section:
a. Click **Update Cache Now** to start the security cache update process.

While the update is ongoing, you can click the [Monitor Update Progress] link that appears to go to the Mirrors page where you can monitor the security cache update progress reported by a percentage value for each mirror.

Note: In the CES Console, a message similar to the following one appears, allowing you to monitor the security cache update progress:

> Updating security cache (10%). Processed security items: 351515/3498585

When the update is completed, the line changes to:

> Done updating security cache.

b. In rare cases where one or more of your sources uses late-binding, click **Clear External Security Cache Now** when you want to reset the external security cache to ensure that permissions for all queries are up-to-date.

CES starts rebuilding the cache from scratch using security providers to ask repositories the permissions for all late-binding source documents matching incoming queries.

In the CES Console, the following message appears:

> The External Security Cache was cleared.

Note: You can enable late-binding for a source from its **Permissions** page.

### 8.6.3.2.4 Disabling or Enabling Queries

You can manually disable and re-enable queries. When disabled, the index no longer returns results to queries sent by end-users from Front-End servers. Disabling queries could be used in extreme cases where you absolutely need more CPU resources available for indexing and can afford to turn off the search service for your end-users.

Note: Queries are always served to members of the System Administrators role, even when the queries are disabled as described in this topic (see "About Administration Roles" on page 406).

To disable or enable queries

1. On the Coveo server, access the Administration Tool.
2. Navigate to the **Details** page (Status > Details).
3. In the **System State** section, next to the **Queries are [current_state]** status, click [Disable] or [Enable].
8.6.3.2.5 Disabling or Enabling Indexing

You can manually disable and re-enable indexing to pause crawlers. While disabled, the index is no longer being updated but can still return results for incoming queries.

It is recommended to disable indexing while you modify connector parameters to ensure no source using the modified connector are being indexed. Temporarily disabling indexing can also be useful to devote maximum CPU resources to querying when querying and indexing processes fight for CPU.

To disable or enable queries

1. On the Coveo server, access the Administration Tool.
2. Navigate to the Details page (Status > Details).
3. In the System State section, next to the Indexing is [current_state] status, click [Disable] or [Enable].

8.6.4 Administration Tool - Index Tab

This section regroups topics that are useful to configure the Coveo Platform Back-End unified index. The Index tab menus allow you, among other things, to manage sources, perform search experience optimization, and manage search scopes.

8.6.4.1 About the Index

The unified index is the heart of the Coveo Platform Back-End. The index contains references to the whole content of indexed documents from the crawled repositories.

Facts about the index:

- The index is organized in source and collections.
- The index records the occurrences and positions of all term variants including those containing accented characters and all small common words.
- The index records the presence in documents of terms with casing variants (first, all, or some letters in uppercase) or special formatting (bold, italic, underline,...) but does not record their positions.
- The index detects and saves the encoding and the language of each indexed document for a large number of languages.
- At query time, the index expands queried terms using language-specific stemming algorithms to return a more complete set of results. You can configure which language to use to perform the expansion (see “Configuring the Culture of a Search Hub With the .NET Interface Editor” on page 550).
- The index maintains a word correction lexicon that sorts indexed terms by their number of occurrences and is used by the query spelling suggestion algorithm to find more frequent spelling variants and propose a correction.
- The index minimizes possible stemming errors by calculating a correlation factor between the searched term and every possible expansion. In search results, documents containing highly correlated expansions are ranked higher than ones containing poorly correlated expansions.
Example: When you search for universe, because of the way the stemming algorithm works, the index expands your query using terms from the univer stem classes that can include university. When the terms universe and university rarely co-occur in your indexed documents, documents containing university are ranked lower.

Note: Correlation computations are performed during off-peak hours for queried terms. You can however launch this calculation from the Administration Tool (see "Modifying or Using Advanced Index Parameters" on page 366).

- The index can process wildcards within phrase searches and when using the NEAR operator. You can enable/disable the possibility to use wildcard within queries (see "Modifying or Using Advanced Index Parameters" on page 366).

- The index continuously and automatically cleans up references to deleted documents (see "About the Index Self-Optimization Process" on page 270).

8.6.4.2 About the Index Self-Optimization Process

The index optimization is a process during which Coveo Enterprise Search (CES) consolidates the index content. The optimization process recycles orphan identifiers from deleted documents and terms to optimize the index structure for faster queries.

The Coveo Platform 7 index features a self-optimizing process that continuously and automatically manages this index compaction. The self-optimization process does not require additional index hard disk space.

The self-optimization index process performs the following tasks:

- Monitors identifiers (DocID, PersistentDocID, TermID) that become available when documents or terms are deleted from the index.

- At each transaction, when a minimum number of orphan identifiers to recycle are available:
  
  - For each identifier, clears any remaining references to the identifier and reassigns the identifier to the pool of identifiers that can be used for new documents/terms.

  The identifier recycling respects processing time and percentage limits to prevent overloading the indexing process. The limits are less restrictive during off-peak hours, allowing for a more aggressive self-optimization process when more Coveo server resources are available.

  Note: You can define the off-peak hours for your Coveo system (see "Modifying System Schedules" on page 439).

  - Issues a message in the CES logs indicating the percentage of recycling performed.

Note: With the assistance of the Coveo Support, it is also possible to fine tune the behavior of the self-optimizing process by modifying the default value of associated parameters in the CES configuration file ([Index_Path]\Config\Config.txt).

In the case of Coveo instances with distributed indexes, the self-optimization process runs independently on each slice and on each mirror.
You can monitor the self-optimizing index process by looking at its messages appearing in the CES Console (see "Using the CES Console" on page 246)

8.6.4.3 About Foreign Keys

**CES 7.0.5388+ (April 2013)**

The foreign key feature allows the Coveo index to manage relations between fields. Index foreign keys allow to relieve connectors from managing the field parent/child relationships.

In a system where a document contains a field that is an ID to another document, it is often needed to be able to index the referenced document, not the ID. It is also needed to be able to know when a referenced item changes so that the parent can be updated in the index on the next incremental refresh, even when the parent content did not change. A foreign key addresses these needs.

**Example:** In Salesforce, the account name may be available only in the Accounts documents. Only the Account ID is set on account children such as opportunities or cases. By setting an Account to Name foreign key relationship, at query time, you can query for @syssfaccountname==ACompanyName and find matching documents even when they do not have the syssfaccountname field but have the syssfaccountid field. The link is made under the hood, in a seamless manner. Also, the syssfaccountname field can be put on the results for display, if needed.

```xml
<ForeignKeys>
  <ForeignKey ID="123">
    <KeyField>syssfaccountid</KeyField>
    <ValueField>syssfaccountname</ValueField>
    <FreeTextSearch>true</FreeTextSearch>
  </ForeignKey>
</ForeignKeys>
```

Foreign keys also support sub-string matches.

**Example:** If an account name is "Government of Canada", the query @syssfaccountname=Canada returns this account as well as any other accounts with Canada in the account name.

The FreeTextSearch option, when set to true allows end-users to also search the content of the FreeTextSearch value fields.

**Example:** Again, if an account name is "Government of Canada", with the FreeTextSearch option set to true, entering Canada in the search box returns this account, even when the term Canada is only present in the foreign key value field.

The foreign key relationship can also be used by facets or ListFacetFieldValues using a look up field. You can build the facet on the syssfaccountid field that is set on all documents and have the syssfaccountname field displayed instead, even when this field is only set on a very small subset of documents.

The foreign key feature works seamlessly across two index slices so that when an account and a related opportunity are stored in different index slices, the look up works.
Note: CES 7.0.6424+ (February 2014) Foreign keys support multiple key fields mapping to a single value field.

Example: A travel website, contains the AirportName field set on Airport records as well as the DepartureAirportID and ArrivalAirportID fields set on Flight records.

When you search for @airportname=gaulle assuming to find all documents related to the Charles de Gaulle Paris Airport (which ID is 9), the search must be:

@airportname=gaulle OR @DepartureAirportID=9 OR @ArrivalAirportID=9.

The following foreign key definition for multiple key field mapping to a single value field allows to automatically return the expected results for the @airportname=gaulle query:

```xml
<ForeignKey ID="1">
  <KeyField>departureairportid</KeyField>
  <ValueField>airportname</ValueField>
</ForeignKey>
<ForeignKey ID="2">
  <KeyField>arrivalairportid</KeyField>
  <ValueField>airportname</ValueField>
</ForeignKey>
```

Limitations

- Currently, the foreign key configuration must be done manually. Because, such configuration may have important advert consequences, you must contact Coveo Support for assistance to set up foreign keys.

- Both the key and value fields must be:
  - String type
  - facet field

- Wildcard matches are not supported.

  Example: The query @syssfaccountname=Cana* will not work.

- Foreign key relationships are not specific to a source or a collection. When the key and value field names are common, the foreign key relation applies to any source in which these fields are present.

- For very high cardinality fields (field having more than one million distinct values), the initial start of the index can take a minute or more. New values are added through the secondary commit, so in the worst case scenario, an ID gets its value mapped about two 2 minutes after indexing is done.

8.6.4.4 About Index Resilience

CES 7.0.6942+ (August 2014)

The Coveo index includes an error resilience feature to prevent stopping and restarting the CES service for potentially temporary error conditions.
**Example:** Index files may be locked while they are scanned by an anti-virus software (which by the way is not a good practice, see "CES and Anti-Virus Software" on page 232) or defragmented by a Windows process. A non-fatal error occurs when a locked file needs to be modified for a transaction. Other attempts to process the transaction will be made on the next commits during which the file will most likely no longer be locked, allowing the transaction to be committed without interrupting the CES Service.

When a non-fatal error occurs during the application of a transaction, rather than immediately stopping the CES service, only a mini core dump file is created ([CES_Path]\CoreDumps\CESService7_nnnn_yymmdd_hhmss_mini.dmp) thus only shortly pausing the index processes as well as saving disk space and processing resources.

A few attempts to perform the process that caused the error are made:

- When the error condition no longer exist, the operation goes through and the CES Service is not interrupted.
- When the error condition persists, the CES process is stopped and a core dump file created ([CES_Path]\CoreDumps\CESService7_nnnn_yymmdd_hhmss_full.dmp). The CES Service must be immediately restarted by the Windows Service Control Manager (default configuration).

When a non-fatal error is detected, the index resilience feature writes the following error messages in the CES Console and in the logs:

- Unexpected non-fatal exception X in thread Y
- An unexpected exception occurred while processing a transaction. The transaction processing will restart X more time(s) with the next index commit(s).

**8.6.4.5 Query Correction Feature**

The Coveo index includes the automatic query correction or *Did You Mean* feature used to detect and automatically suggest or correct misspelled keywords. This topic describes in more detail how this feature works so that you can better understand what it can and cannot do.

Query correction feature facts:

- The query correction is based on a word corrector lexicon (WCL) that contains frequent words and their number of occurrences gathered when documents are indexed, so the spelling suggestions/corrections are based on the index content, not on predefined or custom dictionaries. You can however influence the lexicon algorithm (see "Influencing the Word Corrector Lexicon Algorithm " on page 275).

**Tip:** You can manually update the WCL from the Administration Tool by clicking the Rebuild Word Corrector Lexicon link (see "Modifying or Using Advanced Index Parameters" on page 366).

- The query correction suggestions/corrections improve as the size of the index increases.
- The index must have a minimum size of 2000 documents to start providing query correction suggestions.
- The query correction algorithm is triggered when the query returns a low number of results relative to the size of the index.
**Note:** Query correction suggestions are provided when the index:

- Contains between 2000-10000 documents and returns less than 1000 results following a user query.
- Contains between 10000-50000 documents and returns less than 1250 results following a user query.
- Contains more than 50000 documents and returns less than 0.75% of its results following a user query.

**Example:** For a 1 million documents index, the query must return less than 7500 results for suggestions to be provided.

- Suggestions are not provided if the query has been expanded by the thesaurus.

**Note:** The query correction and the thesaurus are completely independent features (see "Thesaurus Best Practices" on page 331).

- The algorithm is not applied to search terms meeting one or more of the following rules:
  - Containing 3 characters or less
  - Containing a wildcard character (* and ?)
  - Beginning with a number

- An indexed word is not suggested by the word corrector lexicon if the word meets one or more of the following rejection rules:
  - Containing more than 4 numbers.
  - Containing 7 or more consecutive consonants
  - Containing 6 or more consecutive vowels
  - Containing an invalid number of consecutive vowels considering the document language.

**Note:** The rule applies only to the following languages: English, French, Spanish, and German.

**Note:** These word rejection rules are all active by default, but they can be turned off independently to fine tune the query correction behavior. Contact Coveo Support for assistance if you want to do that.

- The query correction is done on a word by word basis, so the correction of a word is not modified by other words in the query.

- A suggested word must have a high degree of similarity (edit distance) with the searched word, i.e., a minimized number of character permutations differentiating it from the original word. A missing or added character is considered a permutation. The edit distance for compatible permutations (such as k replaced by q) is smaller than for an incompatible permutation (such as x replaced by r).

- For a word to be suggested, for each permutation, it must have a number of occurrences in the index that is at least an order of magnitude greater than the original word.
Example: A user inverts two characters in a keyword such as typing `enterprise` rather than correct `enterprise`. Because there are two permutations between the wrong and correct spelling, `enterprise` must have at least two order of magnitudes (100 times) more occurrences in the index than `enterprize` to be suggested as a correction.

- The suggested spelling of a query word is determined based on both the frequency of the alternative words in the lexicon (the higher the better) and their degree of similarity with the original word (the closer the better). Thus, with two alternative spellings having the same edit distance, the word that is more frequent in the index is suggested.

- As an administrator, you can configure how the search interfaces take advantage of the query corrections:
  - For the Coveo .NET Front-End, you can set the search interface default Did You Mean preference (see "Modifying Default .NET Search Interface Preferences" on page 627).
  - For the Coveo JavaScript Search, you can include suggestions or not in a search interface (see DidYouMean Component).

8.6.4.5.1 Influencing the Word Corrector Lexicon Algorithm

The Word Corrector Lexicon (WCL) that powers the Query Correction (Did You Mean) feature can be influenced by a bias file, containing word/bias pairs (see "Query Correction Feature" on page 273).

Example: You add your product names in the bias file to ensure your products are suggested when a client misspelled them in the search box of your e-commerce site. Before your changes, the Did you Mean feature was only suggesting common English words with a high degree of similarity.

To influence the Word Corrector Lexicon Algorithm

1. Ensure your CES index meets the requirements of the Query Correction feature (see "Query Correction Feature" on page 273).

2. List the DidYouMean suggested terms that you want to influence along with their number of occurrences in your index.

   Tip: You can misspell one or two letters in important concepts for your organization and ensure the DidYouMean suggestions are correct.

3. Create a `WordCorrectorBias.txt` file that respects the following format:

   Word1 [-]n
   Word2 [-]n
   Wordn [-]n

   Note: The numbers (n) next to the terms represent the bias in absolute numbers of occurrence in the lexicon. A negative value will decrease the number of occurrences and thus reduce the chance of seeing the term as a DidYouMean suggestion. A positive value will, on the contrary, enforce the term as a possible suggestion. The number of occurrences to add or subtract is dependent on the index content.
4. In the CES 7 config.txt file (located in the C:\CES7\Config folder), in the PhysicalIndex section, add the WordCorrectorBiasFilePath tag with the path to the WordCorrectorBias.txt file.

Example:
<WordCorrectorBiasFilePath>C:\CES7\Config\WordCorrectorBias.txt</WordCorrectorBiasFilePath>

Note: You can also make the algorithm outputs suggestions containing ligated characters, which is impossible otherwise, since the index does not contain any ligated character.

Example: To make the index outputs the "Œsophage" suggestion, you add the term with a bias of 0 (for the term to have the same number of occurrences as "oesophage"):

Œsophage 0

5. Restart the CES service.

6. Once you are satisfied with your bias file, rebuild the Word Corrector Lexicon to make sure the WordCorrectorBias.txt file is used:
   a. On the Coveo server, access the Administration Tool.
   b. Select Index > Advanced.
   c. In the Advanced page, click Rebuild Word Corrector Lexicon.

8.6.4.6 Administration Tool - Sources and Collections Menu

You make content searchable by creating collections of sources of various types.

Note: The parameters available in the various Administration Tool source pages may vary depending on the type of source. Refer to the appropriate source creation topic for more information.

8.6.4.6.1 What Is the Difference between a Collection and a Source?

Collections and sources are subdivisions of the index. Collections are groups of sources built around a theme (ex.: Human Resources and R&D collections); whereas, sources are groups of documents from a single repository (ex.: all documents from the Coveo website). Each collection and source has its own security permissions, meaning that it is possible to limit their access to subgroups of users.
**Example:** The *Human Resources* collection can be accessed only by HR employees, while the *Salaries* source within it can be accessed only by the directors of that department. Example of the index structure:

![Diagram of index structure]

**Note:** Users cannot query a source unless they have access to its parent collection and cannot query a document unless they have access to its parent source.

### 8.6.4.6.2 Adding a Collection

Collections are groups of sources built around a theme. Each collection has its own security permissions which override those of sources, meaning that users can never query the content of a source without having access to its parent collection.

To add a collection:

1. On the Coveo server, access the Administration Tool.
2. Access the **Sources and Collections** page (Index > Sources and Collections).
3. In the **Collections** section, click **Add**.

**Note:** CES 7.0.5425+ (May 2013) You can also duplicate a collection (see "Applying an Action to a Collection or a Source" on page 283). Duplicating a collection is useful when you need to create a collection that contains sources that are similar to the ones of an existing collection.

4. In the right panel, under **Add Collection**:
a. In the **Name** box, enter a name to identify the collection.

This name may be visible by end-users in search interfaces. It can appear in optional **Collection** facets or collection check boxes appearing below the search box, both allowing end-users to refine results by collection. Consequently, choose the name carefully so that it clearly describes the collection content from the end-user point of view. It is also a best practice to ensure that this name follows a similar naming convention as the name of other existing collections.

**Note:** You can always rename a collection but this requires rebuilding all the sources contained in the collection (see “Renaming a Collection” on page 278).

b. Select the appropriate **Allowed Users** option:

- **Everyone**
  
  Grants access to all users.

- **The collection creator**
  
  Grants access only to the administrator who created the collection. This option is useful to test a collection before making it available to end-users.

- **The following users or groups**
  
  Grants access to the users or groups whose accounts are entered in the box. Specify user and group names in the `domain\username` format. Use semicolons to separate entries.

c. Click **Save** to create the collection.

### 8.6.4.6.3 Renaming a Collection

Collections are groups of sources built around a theme. Once a collection is created, you can change its name at any time.

**Important:** Renaming a collection requires rebuilding all the sources contained in the collection.

To rename a collection:

1. On the Coveo server, access the Administration Tool.

2. In the Administration Tool, select **Index > Sources and Collections**.

3. In the **Sources and Collections** page:

   a. In the **Collections** section, expand the drop-down list of the collection for which you want to change the name, and then select **Edit General Properties**.
b. In the right panel, under General, in the Name box, enter the new name for the collection.

**Note:** Remember that this name may be visible by end-users in search interfaces. It will appear in optional Collection facets or collection check boxes below the search box, both allowing end-users to refine results by collection. Consequently, choose the name carefully so that it clearly describes the collection content from the end-user point of view. It is also a best practice to ensure that this name follows a similar naming convention as the name of other existing collections.

c. Click Save.

4. At an appropriate time, rebuild the sources of the renamed collection for the modification to take effect:

   a. In the Collections section, expand the drop-down list of the collection for which you want to change the name, and then select Rebuild All Sources.

   b. Open the CES Console to monitor rebuilding of the sources (see "Using the CES Console" on page 246).

8.6.4.6.4 Modifying Collection Permissions

Collections are groups of sources built around a theme. Each collection has its own security permissions which override those of sources, meaning that users can never query the content of a source without having access to its parent collection. You can modify the collection permissions at any time.

**Note:** Changing the permissions of a collection does not require the rebuild of the sources contained in the collection.

To modify the permissions of a collection

1. On the Coveo server, access the Administration Tool.
2. In the Administration Tool, select **Index > Sources and Collections**.

3. In the **Sources and Collections** page:

   ![Image of Sources and Collections page with Permissions section highlighted]

   a. In the **Collections** section, expand the drop-down list of the collection for which you want to set the permissions, and then select **Edit Permissions**.

   b. In the right panel, under **Permissions**:
      
      - To grant access to the collection:
        
        i. In the **Permissions** section, select the **Specific users** radio button.
        
        ii. In the **Allowed Users** section, click **Add**.
        
        iii. In the **Add identity** dialog box that appears:

          A. In the first drop-down list, select the security provider in which the user or group is defined.

          B. In the **Type** drop-down list, select between three identity types (**User**, **Group**, or **Virtual Group**).

          C. In the **Name** box, enter the account name of the user or group.

          D. Click **Add**.

      - To revoke access to the collection for an account that is listed in the **Allowed Users** box, click the X icon next to the account.
Tip: When you want to revoke the access to more than one account, select the accounts check box, and then click Remove.

- To revoke access to the collection for an account that is not listed in the Allowed Users box, in the Denied Users section:
  
  i. In the Permissions section, select the Specific users radio button.
  
  ii. In the Denied Users section, click Add.
  
  iii. In the Add identity dialog box that appears:

    A. In the first drop-down list, select the security provider in which the user or group is defined.
    
    B. In the Type drop-down list, select between three identity types (User, Group, or Virtual Group).
    
    C. In the Name box, enter the account name of the user or group.
    
    D. Click Add.

Note: The permissions are immediately changed in the index and are immediately applied for new incoming queries.

8.6.4.6.5 What Should Be the Size of a Collection?

The size of a collection is unimportant. What is important is the theme around which it is built, because selecting the collections to search is the first query refinement step. To be effective, each collection must contain documents pertinent to its theme and nothing else.

Example: You can create collections intended for specific departments (such as: Human Resources, R&D, and Sales).

8.6.4.6.6 Adding a Source

A source is a division of the index regrouping all documents indexed from a single repository.

To add a source

1. On the Coveo server, access the Administration Tool.
2. Access the Sources and Collections page (Index > Sources and Collections).
3. In the Sources section, click Add. The Add Source page is displayed.
4. In the Name box, enter a name to identify the source.
5. In the Source Type drop-down list, select the type of repository to crawl.

Note: The available source types correspond to the available connectors (see "Coveo Platform Connectors" on page 734).

6. Select the appropriate source parameters.
7. Click **Save** to create the source without starting the indexing process. This option allows to modify the source properties prior to indexing.

OR

Click **Save and Start** to create the source and start the indexing process with the default properties.

The **Status** page appears.

**Note:** For CES to recognize non-Windows security permissions, security providers must be created (see "Adding or Modifying a Security Provider" on page 417).

### 8.6.4.6.7 Toggling Live Monitoring for a Source

Some repository types can detect that a document was added, modified or deleted and notify external systems. The File connector uses this technique called *live monitoring* to maintain the index up-to-date with the source content. When supported, live monitoring is enabled by default. You can however manually enable or disable live monitoring.

**To toggle live monitoring for a source**

1. On the Coveo server, access the Administration Tool.

2. Access the **Sources and Collections** page (Index > Sources and Collections).

3. In the **Collections** section, click the collection that contains the source for which you want to toggle the live monitoring state.

4. In the **Sources** section, click the appropriate source.

5. On the horizontal button bar:

   - When live monitoring is active, click **Disable Live Monitoring** to turn it off.

   **OR**

   - When live monitoring is turned off, click **Enable Live Monitoring** to activate it.
8.6.4.6.8 Applying an Action to a Collection or a Source

In the Sources and Collections page of the Administration Tool, the More Action drop-down list regroups actions that you can apply to selected collections or sources.

The following table describes the available actions.

<table>
<thead>
<tr>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rebuild</td>
<td>Re-indexes the content and permissions of all the documents from the repository, even those that have not been modified since the last indexing date.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> Rebuilding sources requires more time and CPU resources than refreshing them; however, it is a thorough process that ensures all documents are updated in the index.</td>
</tr>
<tr>
<td>Full Refresh</td>
<td>Re-scans all documents from the repository, but re-indexes the content and permissions only for the documents that are found to be new, modified, or deleted since the last rebuild, full refresh, or incremental refresh.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> Refreshing sources requires less time and CPU resources than rebuilding them and is recommended to update the index on a daily basis. However, erroneous modification dates can keep CES from refreshing documents. If you identify that specific documents are not up-to-date, rebuild the source.</td>
</tr>
<tr>
<td>Incremental Refresh</td>
<td>Re-scans and re-indexes content and permissions only for documents that the repository reports as new, modified, or deleted since the last rebuild, full refresh, or incremental refresh.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> The incremental refresh is available only for sources associated with repositories that have the ability to retrieve the list of documents that have changed since a specific point in the past.</td>
</tr>
<tr>
<td>Pause</td>
<td>Suspends the refreshing or rebuilding process temporarily. The Pause action is used to free CPU resources in order to speed up other refreshes and rebuilds.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong> Fifteen (15) sources are being refreshed concurrently and CES is slowed down. Use the Pause option to pause half of them (or more) to regain speed.</td>
</tr>
<tr>
<td>Resume</td>
<td>Restarts the paused refresh or rebuild. Note that stopped actions cannot be resumed.</td>
</tr>
<tr>
<td>Stop</td>
<td>Cancels the refreshing or rebuilding process. Note that a stopped process cannot be resumed.</td>
</tr>
<tr>
<td>Disable Live</td>
<td>For File sources, disables automatic re-indexing of documents identified as modified by Windows file system events (see &quot;About Incremental Refresh and Live Monitoring&quot; on page 308).</td>
</tr>
<tr>
<td>Monitoring</td>
<td></td>
</tr>
<tr>
<td>Enable Live</td>
<td>For File sources, enables automatic indexing of newly created, modified, or deleted documents identified by Windows file system events (see &quot;About Incremental Refresh and Live Monitoring&quot; on page 308).</td>
</tr>
<tr>
<td>Monitoring</td>
<td></td>
</tr>
<tr>
<td>Action</td>
<td>Description</td>
</tr>
<tr>
<td>--------</td>
<td>-------------</td>
</tr>
<tr>
<td>Duplicate</td>
<td>Reproduces the configuration of selected collections or sources. This action is useful to more quickly configure similar sources/collections and then only perform minor customization on the duplicated source/collection. You must then rebuild the new sources to index their content. When you duplicate a collection, the new collection is created with the name <strong>Copy of [original_collection_name]</strong> that you can edit. The configuration of the sources in the original collection are also copied with their original names and assigned to the new collection. <strong>Example:</strong> When you want to create development, staging, and production collections.</td>
</tr>
<tr>
<td>Delete</td>
<td>Eliminates selected collections or sources and their content from the index.</td>
</tr>
</tbody>
</table>

**Notes:**

- If an action is applied to a collection, then it is also applied to all its sources.
- A Rebuild, Full Refresh, or Incremental Refresh will not take into account changes made to security groups of the indexed repository (see "Refreshing Security Caches" on page 266).

To apply an action to a collection or a source

1. On the Coveo server, access the Administration Tool.
2. In the Administration Tools, select **Index > Sources and Collections**.
3. In the **Sources and Collections** page:

   a. In the **Collections** section, select the check box for one or more collections on which you want to apply an action.

       OR

   b. In the corresponding **More Actions** drop-down list, select the action that you want to apply.
The statuses of the sources are modified accordingly (see "What Are the Possible Statuses of a Source?" on page 285).

**Note:** Refreshing or rebuilding whole collections can slow down CES. If this occurs, refresh sources individually.

### 8.6.4.6.9 Incremental Refresh vs Full Refresh vs Rebuild

Once a source is created, you can schedule or manually apply the following action types to maintain the source up-to-date with the repository or to apply source configuration changes (see "What Should Be The Frequency of Source Refresh Schedules?" on page 441).

#### Incremental Refresh

An incremental refresh scans and re-indexes content and permissions only for documents identified by the repository as new, modified, or deleted since the last rebuild, full refresh, or incremental refresh.

Whenever available, schedule incremental refreshes at short intervals to constantly and efficiently maintain your source up-to-date with the repository content (see "Scheduling a Source Incremental Refresh" on page 433).

**Note:** The incremental refresh of some source types may have some limitations (often due to repository API limitations). Refer to the appropriate Coveo connector documentation for details.

#### Full Refresh

A full refresh re-scans all documents from the repository. It re-indexes the permissions of all documents and re-indexes the content only for the ones that are found to be new, modified, or deleted since the last rebuild, full refresh, or incremental refresh.

When incremental refresh is not available or has some limitations, or as a safety net, schedule full refreshes at appropriate intervals to maintain your source up-to-date with the repository content (see "Scheduling Source Refresh Actions" on page 435).

**Note:** The full refresh of the Web Page connector does not catch deleted pages. A rebuild is necessary to eliminate deleted web pages from the index.

#### Rebuild

A rebuild completely re-indexes the content and permissions of all the documents from the repository, even those that have not been modified since the last indexing date.

You must rebuild a source when you change its configuration. For large sources, plan your changes to minimize the number of rebuilds and the impact of the Coveo server resources (see "Applying an Action to a Collection or a Source" on page 283).

Apart from cases where a full refresh cannot fully keep a source up-to-date with the repository content, it is not recommended to schedule rebuilds, particularly for large sources.

### 8.6.4.6.10 What Are the Possible Statuses of a Source?

The status of a source indicates the type of action (if any) performed on the source at the moment.
### Status | Description
---|---
Not Started | Indicates that the content has not been indexed because, at source creation, the Save button is clicked instead of the Save and Start one (see "What Is the Difference between Save and Save and Start?" on page 286).
Idle | Indicates that the content is indexed and no action is being performed on the source.
Indexing | Indicates that the content is being indexed for the first time.
Rebuilding | Indicates that all the documents are being re-indexed.
  **Note:** Rebuilding sources requires more time and CPU resources than refreshing them; however, it is a thorough process which makes sure all documents are updated.
Refreshing | Indicates that documents modified since the previous indexing date are being re-indexed.
  **Note:** Refreshing sources requires less time and CPU resources than rebuilding them and is recommended to update the index on a daily basis. However, erroneous modification dates can keep the Coveo Platform from refreshing documents. Therefore, if the index history report displays an abnormally low number of updates (ex.: 100 updates for a frequently modified source containing 100,000 documents) it is recommended to rebuild the source.
Paused | Indicates that the refreshing or rebuilding process is temporarily suspended. The Pause action is used to free CPU resources in order to speed up other refreshes and rebuilds.
Pending (crawlers are stopped) | Indicates that the refreshing or rebuilding process has been started but cannot be carried out because indexing is disabled. Pending can be used because the number of threads for the connectors is smaller than the number of sources to refresh for the same connector.
  **Note:** To enable indexing, access the Details page (Status > Details) and click [Enable] beside Indexing is disabled in the System State section.

#### 8.6.4.6.11 What Is the Difference between Save and Save and Start?

Clicking **Save and Start** at the end of source creation (see "Adding a Source" on page 281) automatically launches the indexing process; whereas, clicking **Save** creates the source with the specified configuration but does not launch the indexing process. The purpose of the Save function is to allow the modification of source parameters prior to indexing. To launch the indexing process after clicking **Save**, rebuild the source (see "Applying an Action to a Collection or a Source" on page 283).
8.6.4.6.12 What Should Be the Size of a Source?

The size of a source may become a problem when it takes significant time to refresh or rebuild it. A source containing thousands of large documents can take hours to rebuild. Although the refreshing or rebuilding process does not prevent users from querying the source, it requires considerable CPU resources. Therefore, CES can be slowed down for several hours each day because of re-indexing. Creating smaller sources allows to distribute the refreshing or rebuilding process over the week or even the month.

Example: You can index the intranet of a company in three different sources—the first one can contain documents that are updated daily (ex.: project schedules), the second one documents updated once every few weeks (ex.: financial reports) and the third one documents rarely updated (ex.: documentation concerning previous versions of the product). Therefore, you can distribute the re-indexing process by refreshing the first source daily, the second one weekly and the third one monthly.

Note: The size of the index is limited by the license type. If a license allows the indexing of 100,000 documents, the total size of sources cannot exceed this number.

8.6.4.6.13 What Are the Source Properties?

The source properties are additional parameters which can be defined before or after a source is indexed.

To display the source property pages

1. On the Coveo server, access the Administration Tool.
2. In the Administration Tool, select Index > Sources and Collections.
3. In the Sources and Collections page:
a. In the **Sources** section, expand the appropriate source drop-down list.

b. Select the appropriate property. Its corresponding page is displayed. The following table describes the source property pages.

<table>
<thead>
<tr>
<th>Property</th>
<th>Applies to</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>View Status</td>
<td>All sources</td>
<td>Displays general information concerning the content of the source and actions performed on it (see &quot;What Information Is Displayed in the Status Page?&quot; on page 289).</td>
</tr>
<tr>
<td>Edit General Properties</td>
<td>All sources</td>
<td>Displays the properties of the source and allows their modification (see &quot;Modifying General Source Parameters&quot; on page 292). <strong>Note</strong>: Most properties displayed in the <strong>General Properties</strong> page are defined during source creation (see &quot;Adding a Source&quot; on page 281).</td>
</tr>
<tr>
<td>Edit Filters</td>
<td>All sources except Manual Crawler</td>
<td>Displays the inclusion and exclusion filters applied to the source and allows their modification (see &quot;Adding or Modifying Source Filters&quot; on page 295).</td>
</tr>
<tr>
<td>Edit Refresh Schedule</td>
<td>All sources except Manual Crawler</td>
<td>Displays the refresh schedule used to update the source and allows to select a different one (see &quot;Scheduling Source Refresh Actions&quot; on page 435).</td>
</tr>
<tr>
<td>Edit Fields</td>
<td>All sources</td>
<td>Displays the field set used to index the source and allows to select a different one (provided custom sets have been created).</td>
</tr>
</tbody>
</table>
### Property | Applies to | Description
--- | --- | ---
Edit XML Document Definition | All sources | Displays the XML document definition used to index the source and allows to select a different one. **Note:** The Coveo Platform does not provide built-in XML document definitions but you can add one (see "Adding an XML Document Definition" on page 508).

Edit SharePoint | SharePoint | Displays the SharePoint reference set used to index the source and allows to select a different one (provided custom sets have been created).

Edit Lotus Notes | Lotus Notes | Displays the Lotus Notes form set used to index the source and allows to select a different one (provided custom sets have been created).

Edit Document Types | All sources | Displays the document type set used to index the source and allows to select a different one (provided custom sets have been created).

Edit Conversion Scripts | All sources | Displays the preconversion and postconversion scripts used to index the source and allows to select different ones. **Note:** Conversion scripts have to be written in VBScript or JScript and added to CES (see Conversion Scripts).

Edit Permissions | All sources except Manual Crawler | Displays the source permissions and allows their modification (see "Modifying Source Security Permissions" on page 297).

Edit Forms | Web Pages | Allows the configuration of forms used by the Web connector to access secure pages (see "Indexing Secure Web Pages Using Forms" on page 300).

Refresh Documents | Local/Network Files Web Pages | Allows to refresh, add or remove a single file or folder (see "Managing Single Documents Within Local/Network or Web Sources" on page 303).

Edit Advanced | All sources | Allows the modification of the advanced parameters of a source (see "Modifying Advanced Source Parameters" on page 305).

---

#### 8.6.4.6.14 What Information Is Displayed in the Status Page?

In the Administration Tool, the **Status** page for a source displays general information concerning the content of a source and actions performed on it.

To display the Status page of a source

1. On the Coveo server, access the Administration Tool.

2. In the Administration Tool, select **Index > Sources and Collections**.

3. In the **Sources and Collections** page:
a. In the **Sources** section, expand the appropriate source drop-down list.

b. Select **View Status**.
The following table describes the content of the sections in the **Status** page.

<table>
<thead>
<tr>
<th>Section</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Status</strong></td>
<td>Displays the status of the source (see &quot;What Are the Possible Statuses of a Source?&quot; on page 285).</td>
</tr>
<tr>
<td><strong>Addresses</strong></td>
<td>Displays the addresses at which the connector begins the crawling process.</td>
</tr>
<tr>
<td><strong>Number of Documents</strong></td>
<td>Displays the number of documents contained in the source as well as their total size (see &quot;Administration Tool - Index Content Menu&quot; on page 370). Click [Details] to review the content of this source in the <strong>Index Browser</strong> (see &quot;Reviewing Document Details from the Index Browser&quot; on page 375).</td>
</tr>
<tr>
<td><strong>Last Operation</strong></td>
<td>Displays the duration as well as starting and ending date/time for the last operation performed on the source (i.e. indexing, refreshing or rebuilding) . Click [Details] to access the <strong>Index</strong> page showing the logs for this source (see &quot;What Information Is Displayed in the Index Log?&quot; on page 398).</td>
</tr>
<tr>
<td><strong>Last/Current Operation Statistics</strong></td>
<td>Displays documents crawled during the most recent or current operation according to the type and subtype of action taken. Click [Details] to access the <strong>Index History</strong> page review indexing history for this source (see &quot;What Information Is Displayed in the Index History?&quot; on page 388).</td>
</tr>
</tbody>
</table>
## Section Description

<table>
<thead>
<tr>
<th>Conversion Status</th>
<th>Displays a count of documents waiting to be converted and list documents currently being converted.</th>
</tr>
</thead>
</table>

**Example:** A File connector source is converting documents.

<table>
<thead>
<tr>
<th>Conversion Status</th>
<th>Documents Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>file://MyFileServer/.../delxps m130R ...</td>
<td>0% 100%</td>
</tr>
<tr>
<td>file://MyFileServer/.../administration ...</td>
<td>0% 100%</td>
</tr>
<tr>
<td>file://MyFileServer/.../julstream demo ...</td>
<td>0% 100%</td>
</tr>
<tr>
<td>file://MyFileServer/.../administration ...</td>
<td>0% 100%</td>
</tr>
<tr>
<td>file://MyFileServer/.../administration ...</td>
<td>0% 100%</td>
</tr>
</tbody>
</table>

### 8.6.4.6.15 Modifying General Source Parameters

The **General** page displays some of the properties entered at source creation (see "Adding a Source" on page 281) as well as new ones such as title and metadata name. You can modify these properties after a source has been created and even after its content has been indexed. In the latter case however, you must then rebuild the source.

**Note:** The parameters available in the **Source: [source_name]** General page depend on the type of source. Refer to the appropriate source creation topic for more information.

To modify the general properties:

1. On the Coveo server, access the Administration Tool.
2. In the Administration Tool, select **Index > Sources and Collections**.
3. In the **Sources and Collections** page:
   a. In the **Collections** section, select the collection the source that you want to modify.
   b. In the **Sources** section, select the source that you want to modify.
   c. In the navigation panel on the left, select **General**.
4. In the **General** page:
   a. Modify the appropriate properties. For more information concerning these properties, refer to the following table.
<table>
<thead>
<tr>
<th>Property</th>
<th>Applies to</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>All sources</td>
<td>Indicates the name of the source. It can be modified to avoid confusing two sources or respect naming conventions.</td>
</tr>
<tr>
<td>Source Type</td>
<td>All sources</td>
<td>Indicates the type of the source. It cannot be modified.</td>
</tr>
<tr>
<td>Addresses</td>
<td>All sources</td>
<td>Indicates the address at which the connector began the crawling process. The connector will keep on trying to crawl the source at this address, even if that source is moved somewhere else.</td>
</tr>
<tr>
<td>Rating</td>
<td>All sources</td>
<td>Specifies whether documents from the source should receive a higher or lower ranking than average.</td>
</tr>
<tr>
<td>Options</td>
<td>All sources</td>
<td>Provides additional information on how to index the source and retrieve its documents.</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Index subfolders</strong>: Indexes folders recursively, starting with the main addresses and proceeding to deeper levels until every document is indexed.</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Example</strong>: If <code>\CoveoServer\Help\AdminTool\</code> is the main address and the <code>Index subfolders</code> option is selected, then <code>\CoveoServer\Help\AdminTool\Sources\</code> and <code>\CoveoServer\Help\AdminTool\Sources\Local\</code> are also indexed.</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Index Personal Sites</strong>: Indexes all the personal sites linked to the SharePoint portal. Note that this option is selected by default and applies to SharePoint sources.</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Index subsites</strong>: Indexes subsites recursively, starting with the main addresses and proceeding to deeper levels until every document is indexed.</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Example</strong>: If <code>http://intranet/pages/</code> is the main address and the <code>Index subfolders</code> option is selected, then <code>http://intranet/pages/news/</code> and <code>http://intranet/pages/news/2007/</code> are also indexed.</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Index the document's metadata</strong>: Indexes metadata (ex.: modification date and author of documents).</td>
</tr>
<tr>
<td>Property</td>
<td>Applies to</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------------</td>
<td>------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Document’s addresses are case-sensitive</td>
<td></td>
<td>This option needs to be checked only in rare cases for case sensitive systems in which distinct documents may have the same file name but with different casing.</td>
</tr>
<tr>
<td>Generate a cached HTML version of indexed documents</td>
<td></td>
<td>Produces a Quick View of documents. Note that this option is selected by default and applies to all sources.</td>
</tr>
<tr>
<td>Open results with cached version</td>
<td></td>
<td>Displays the Quick View instead of the actual document when the title of a document is clicked in the result list. The purpose of this option is to open documents that are not available anymore or have never really existed (stored in a database, XML record, documents generated, etc.). Note that Generate a cached HTML version of indexed documents must be selected in order for Open results with cached version to be available.</td>
</tr>
<tr>
<td>Disable document summarization</td>
<td></td>
<td>Disables the creation of a document summary and the extraction of concepts. When selected, CES however takes the first sentences of the document as the summary. The search results summary therefore includes these first sentences but not concepts. This option is not selected by default, but applies to all sources.</td>
</tr>
<tr>
<td>Skip addresses with parameters (domain.com?parameters)</td>
<td></td>
<td>Keeps the Coveo Platform from indexing pages whose addresses contain a query part—the purpose of this option is to only index relevant documents in several copies. This often occurs for certain sites and variables (for example, ID). Another purpose is to save disk space. Note that this option is not selected by default, but applies to Web Pages sources.</td>
</tr>
<tr>
<td>SharePoint Sites Discovery</td>
<td>SharePoint</td>
<td>Specifies which SharePoint sites to index:</td>
</tr>
<tr>
<td>Index only starting addresses</td>
<td></td>
<td>Indexes only the sites whose addresses are entered in the Addresses box.</td>
</tr>
<tr>
<td>Index the starting addresses and all sites listed in the Portal Site Directory</td>
<td></td>
<td>Indexes the sites whose addresses are entered in the Addresses box as well as all sites, related to these addresses, listed in the portal directories.</td>
</tr>
<tr>
<td>Index the web application of the starting addresses</td>
<td></td>
<td>Indexes the content of the virtual directories related to the starting addresses. Note that CES must be integrated to SharePoint; otherwise, the connector is unable to locate virtual directories.</td>
</tr>
<tr>
<td>Index all web applications having the same host name</td>
<td></td>
<td>Indexes the content of all virtual directories related to the starting addresses even if their host headers are different. Note that CES must be integrated to SharePoint; otherwise, the connector is unable to locate virtual directories.</td>
</tr>
<tr>
<td>Title Selection Sequence</td>
<td>All sources</td>
<td>Indicates the sequence followed by CES to determine the title of a document (this title is displayed in the result list). The order of the three options must be defined by clicking the arrows (↑↓). Therefore, if CES fails to extract a title using the first option, it proceeds to the second one and so on.</td>
</tr>
<tr>
<td>Use the title extracted by the converter</td>
<td></td>
<td>The title extracted by the converter is the metadata title.</td>
</tr>
<tr>
<td>Automatically detect the title of documents</td>
<td></td>
<td>The title automatically extracted by the CES converter is made of the same key topics used to produce the excerpt and summary of the document.</td>
</tr>
<tr>
<td>Use the filename</td>
<td></td>
<td>The filename is given to a document when saving it.</td>
</tr>
</tbody>
</table>
### 8.6.4.6.16 Adding or Modifying Source Filters

The starting address of a source determines the content that is crawled while source filters control what is indexed. You can use source filters to more specifically control subsections to index or not under a source starting address. Inclusion/exclusion rules use either wildcard or regular expressions to define filtering patterns.

**Note:** Use the ECMAScript regular expression syntax implemented for example by JavaScript (see Using Regular Expressions with JavaScript).

Exclusion filters are commonly used for any source type to prevent indexing of one or more subsections under the starting address.

**Example:** The starting address of a File connector source for human resources files is file://corp.MyCompany.com/dfs/dept/HR. You can use the following exclusion filter to prevent indexing retired employees documents that are all under the same folder:

```
file://corp.MyCompany.com/dfs/dept/HR/employees/retired/*
```

Inclusion filters are typically used for Web connector sources to include referred web pages outside of the starting address.

**Example:** The starting address of a Web connector source is http://www.MyCompany.com. This website refers to some pages on the related career website (http://career.MyCompany.com) that you want to also index. You can add the following inclusion filter pattern to also index job opportunities:

```
http://career.MyCompany.com/jobs/*
```
**Note:** You can also use inclusion filters with other source types to only index a few subsections under the starting address, but in this case, your source may waste resources by crawling a large number of folders that will not be indexed. The best practice is to rather create one source per subsection, or when the source type allows it, enter more than one starting address for one source.

To add or modify a source filter

1. On the Coveo server, access the Administration Tool.
2. In the Administration Tool, select Index > Sources and Collections.
3. In the Sources and Collections page, select the collection containing the source for which you want to add or modify source filters.
4. In the Sources section, select the source.
5. In the navigation panel on the left, select Filters.
6. In the Filters page:

   ![Filters page](image)

   - To add or modify an exclusion filter:
     a. Click **Add an Exclusion Filter** to create a new filter or click an existing exclusion filter to modify it.
     b. In the **Edit an Exclusion Filter** page, in the **Excluded Patterns** box, enter one or more address patterns (one pattern per line) to exclude using either wildcard characters ( * or ?) or a regular expression.

     Patterns must be subsections of existing inclusion filters otherwise they will be useless.
     c. In the **Type** box, select the search pattern option used in the patterns you entered in **Excluded**
Patterns.

d. Click Save/Apply Changes.

To add or modify an inclusion filter:

Note: Inclusion filters already listed correspond to entries in the Addresses box of the General page. In this box, using a slash or not, at the end of the starting address path for a file system folder (as opposed to a file) as no effect on what is crawled.

It however affects what is indexed with the inclusion filter automatically created for each starting address. When the trailing slash is omitted, the last folder of the starting address is truncated from the inclusion filter.

Example: The starting address file:///C:/temp/ creates the inclusion filter file:///C:/temp/*, while the starting address file:///C:/temp creates the inclusion filter file:///C:/*.

a. Click Add an Inclusion Filter to create a new filter or click an existing inclusion filter to modify it.

b. In the Edit an Inclusion Filter page, in the Allowed Patterns box, enter one or more address patterns (one pattern per line) to include using either wildcard characters ( * or ? ) or a regular expression.

Note: A filter pattern can include a file extension to filter by file type but it is a better practice to define an appropriate document type set for this source (see "Creating a Document Type Set" on page 477).

c. In the Type box, select the search pattern option used in Allowed Patterns.

d. Click Save/Apply Changes.

e. If you are using inclusion filters to index subsections under the starting address:

Note: Using inclusion filters like this can have a significant performance cost. The best practices is to rather create one source per subsection to include, or when the source type allows it, enter more than one starting address for one source.

i. If the default wildcard * inclusion filter is present, select it, and then click Delete to remove it and prevent everything below the starting address to be indexed.

ii. For a File connector source, in the General page, ensure that the Expand Before Filtering option is selected otherwise nothing will be crawled.

iii. For a SharePoint connector source, in the Advanced page, ensure that the Expand sites and lists before applying filter option is selected otherwise nothing will be crawled.

7. Refresh the source for the modifications to take effect.

8.6.4.6.17 Modifying Source Security Permissions

Three levels of security exist in CES index:
- Collection-level security
- Source-level security
- Document-level security

Source-level permissions determine which users have access to a source. By default, sources can be accessed by all users who have access to the parent collection. You can however override these permissions. Even if a user has access to a source, document-level permissions are required to display its content.

**Note:** Source-level permissions are not indexed for Web Pages sources; however, if Web files are stored locally (i.e., on the same network as CES), it is possible to associate file server permissions to them.

This topic contains the following sections:

- "Modifying the permissions" on page 298
- "Mapping the security permissions of a Web source" on page 300

8.6.4.6.17.1 Modifying the permissions

1. On the Coveo server, access the Administration Tool.
2. In the Administration Tool, select **Index > Sources and Collections**.
3. In the **Sources and Collections** page:
   a. In the **Collections** section, select the collection the source that you want to modify.
   b. In the **Sources** section, select the source that you want to modify.
   c. In the navigation panel on the left, select **Permissions**.
4. In the **Permissions** page, in the **Permissions** section, select one of the following options:

**Index security permissions**

Grants access to all users having the appropriate collection permissions. Document-level security is indexed.

**Specify the security permissions to index**

Grants access only to users whose accounts are entered in the **Allowed Users** box. Document-level permissions are not indexed.

**Important:** Because document-level permissions are not indexed, a user added to the **Allowed Users** list that do not have access to a document in the original repository will be able to view its excerpt, summary and Quick View from the search results.

**Index security permissions and specify additional security permissions to index**

Indexes document-level permissions and grants additional access to users whose accounts are entered in the **Allowed Users** box and denies access to users whose accounts are entered in the **Denied Users** box.
Important: The accounts entered in the Allowed Users box override document-level permissions. This means that even users who do not have access to a document are able to view its search result excerpt, summary, and Quick View.

Late Binding

When it is not possible to gather permission information at indexing time, as a last option to support secure search results, select Late Binding to identify which documents a user is allowed to see at query time. With this method, query response time is very slow the first time a query is performed, but much faster on next occurrences.

5. When you selected Specify the security permissions to index or Index security permissions and specify additional security permissions to index, for each user to which you want to modify the source permissions:

   - To grant access to the source, in the Allowed Users section:
     
     i. Enter the account name of the user or group.

     Example: For an Active Directory account, enter the name in the domain\username form.

     ii. Select if the entered name is a User or a Group.

     iii. Select the security provider in which this user or group is defined.

     iv. Click Add.

   - To revoke access to the source for an account that is listed in the Allowed Users box, select the account, and then click Remove.

   - To revoke access to the source for an account that is not listed in the Allowed Users box, in the Denied Users section:

     i. Enter the account name of the user or group.

     Example: For an Active Directory account, enter the name in the domain\username form.

     ii. Select if the entered name is a User or a Group.

     iii. Select the security provider in which this user or group is defined.

     iv. Click Add.

6. Click Apply Changes.
Tip: CES 7.0.5388+ (April 2013) When you add source level permissions, these permissions are automatically assigned to a Custom Source Permissions level that is visible from the Index Browser.

When you add source level permissions, these permissions are automatically assigned to a Custom Source Permissions level that is visible from the Index Browser.

8.6.4.6.17.2 Mapping the security permissions of a Web source

You can map Web Page sources with local files to indexing of document-level security permissions for these sources.

Example: If http://www.coveo.com is mapped with its equivalent folder on \CoveoServer\WebPage\, the permissions granted to the files in the \CoveoServer\WebPage\ folder are also indexed for the Web Pages sources.

1. On the Coveo server, access the Administration Tool.
2. In the Permissions page corresponding to the source is displayed, click Add.
3. In the Edit Web File Security page:
   a. In the Web Address box, enter the address of the Web source.
      
      Example: http://www.coveo.com
   b. In the Network File Path box, enter the path of the folder containing the Web files.
      
      Example: \CoveoServer\WebPage\.
   c. Click Save.

8.6.4.6.18 Indexing Secure Web Pages Using Forms

A website may contain secured Web pages that can only be accessed by filling appropriate information in a form (name, address, etc.). CES must know what information to provide and where to provide it to be able to index these pages.

In the Add Form Configuration page of the Administration Tool, you can retrieve form parameters from websites or enter them manually and configure CES to automatically fill forms for both HTTP and HTTPS forms.

This topic contains the following sections:
8.6.4.6.18.1 Retrieving the form parameters from a website

1. On the Coveo server, access the Administration Tool.

2. In the Administration Tool, select Index > Sources and Collections.

3. In the Sources and Collections page, in the Sources section, expand the drop-down list of the source that you want to modify, and then select Edit Forms.

4. In the Forms page, click Add.

5. In the Add a Form Configuration page:
   a. In the Form Parameters drop-down list, select Get the form parameters from a Web address.
   b. In the Form Address box, enter the URI of the form.
      

   c. Click Retrieve parameters from URL.
The **Form to Use**, **Name**, **Form Address**, **Method** and **Action** are automatically retrieved.

d. Enter the appropriate parameters. For more information, refer to the following table.

<table>
<thead>
<tr>
<th>Section</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Form to Use</td>
<td>Indicates which form to use if the <a href="https://www.coveo.com/">Get the form parameters from a Web address</a> action has encountered more than one form at the specified address.</td>
</tr>
<tr>
<td>Name</td>
<td>Identifies the form.</td>
</tr>
<tr>
<td>Form Address</td>
<td>Indicates the address where the form is located.</td>
</tr>
<tr>
<td>Method</td>
<td>Indicates the method used to submit form information (either Get or Post).</td>
</tr>
<tr>
<td>Action</td>
<td>Indicates the address where the form information is submitted.</td>
</tr>
<tr>
<td>Parameters</td>
<td>Identifies the type, name and value of each parameter. The <strong>Type</strong> parameter indicates the nature of the information; whereas, its <strong>Name</strong> identifies the field in which the <strong>Value</strong> is submitted.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong> To enter Coveo in the <strong>Username</strong> box, the type would be <strong>Text</strong>, the name <strong>Username</strong> and the value Coveo.</td>
</tr>
<tr>
<td></td>
<td>To add parameters, click <strong>Add</strong>.</td>
</tr>
<tr>
<td></td>
<td>The parameter types are:</td>
</tr>
<tr>
<td></td>
<td><strong>Text:</strong> String value entered in a text box (ex.: username).</td>
</tr>
<tr>
<td></td>
<td><strong>Password:</strong> String value entered in a password box. Note that it is replaced by dots (•••) for security reasons.</td>
</tr>
<tr>
<td></td>
<td><strong>Checkbox:</strong> True or false (i.e. selected or unselected) value applied to a check box.</td>
</tr>
<tr>
<td></td>
<td><strong>Radio:</strong> True or false (i.e. selected or unselected) value applied to a radio button.</td>
</tr>
<tr>
<td></td>
<td><strong>Submit:</strong> Submit function applied to previously entered parameters.</td>
</tr>
<tr>
<td></td>
<td><strong>Reset:</strong> Reset function applied to the previously entered parameters.</td>
</tr>
<tr>
<td></td>
<td><strong>File:</strong> File attached to the form.</td>
</tr>
<tr>
<td></td>
<td><strong>Hidden:</strong> Value entered in a hidden box.</td>
</tr>
<tr>
<td></td>
<td><strong>Image:</strong> Image file attached to the form.</td>
</tr>
<tr>
<td></td>
<td><strong>Button:</strong> Button (other than Submit or Reset) clicked.</td>
</tr>
<tr>
<td>Addresses Using This Form</td>
<td>Indicates the addresses accessed using this form. Use wildcards if necessary.</td>
</tr>
<tr>
<td>Failed Authentication Result Addresses</td>
<td>Indicates the address of the page where CES is redirected if authentication fails (instead of indexing the latter page, CES attempts to re-authenticate).</td>
</tr>
<tr>
<td>Options</td>
<td>Indicates whether to re-authenticate each time a secure page is accessed or use authentication cookies. Because re-authentication slows down the indexing process, the <strong>Always authenticate when crawling a document</strong> option should be selected only if the secure pages do not support cookies.</td>
</tr>
<tr>
<td>Test Form</td>
<td>Indicates the address used to test the form. When <strong>Apply Changes and Test the Form Using This Address</strong> is clicked, CES tries to access this page. If it succeeds, the form is considered valid. If it fails, form parameters must be modified.</td>
</tr>
</tbody>
</table>

e. Click **Apply Changes and Test the Form Using This Address** to test the form. If the test fails, verify the validity of each parameter.

f. When the test succeeds, click **Save**.
8.6.4.6.18.2 Entering the form parameters manually

1. On the Coveo server, access the Administration Tool.

2. In the Administration Tool, select Index > Sources and Collections.

3. In the Sources and Collections page, in the Sources section, expand the drop-down list of the source that you want to modify, and then select Edit Forms.

4. In the Forms page, click Add.

5. In the Add a Form Configuration page:
   a. In the Form Parameters drop-down list, select Enter the form parameters manually.
   b. Enter the appropriate parameters. For more information, refer to the table in the previous section.
   c. Click Apply Changes and Test the Form Using This Address to test the form. If the test fails, verify the validity of each parameter.
   d. When the test succeeds, click Save.

Important: Unless Always authenticate when crawling a document is selected, CES keeps authentication cookies in its memory. Therefore, if authentication fails it can be because of expired cookie information delete cookies to force CES to re-authenticate using the form. If this procedure does not solve the problem, the form information has been modified; create a new form.

8.6.4.6.18.3 Deleting the authentication cookies

1. On the Coveo server, access the Administration Tool.

2. In the Administration Tool, select Index > Sources and Collections.

3. In the Sources and Collections page, in the Sources section, expand the drop-down list of the source that you want to modify, and then select Edit Forms.

4. In the Forms page, under Authentication Cookies, click Delete Source Authentication Cookies.

8.6.4.6.19 Managing Single Documents Within Local/Network or Web Sources

You can manually re-index or delete single files or folders within Local/Network Files or Web Pages sources. This process is useful when only a few documents have to be re-indexed and the refreshing or rebuilding process takes more time than manual modifications.

To apply modifications to a single file or folder

1. On the Coveo server, access the Administration Tool.

2. In the Administration Tool, select Index > Sources and Collections.

3. In the Sources and Collections page, in the Sources section, expand the drop-down list of the source that you want to modify, and then select Refresh Documents.
4. In the **Refresh Document** page:

   a. In the **Address** box, enter the path of the file or folder.

   b. In the **Options** section, select either **Refresh/Add to index** or **Remove from index** and select the appropriate check boxes. For more information, refer to the following table.

<table>
<thead>
<tr>
<th>Option</th>
<th>Applies to</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Index documents only if they are modified</td>
<td>Refresh/Add to Index</td>
<td>Re-indexes documents only if they have been modified since the previous indexing date.</td>
</tr>
<tr>
<td>Subfolders or Subsites</td>
<td>All</td>
<td>Indexes or deletes subfolders or subsites recursively.</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Example:</strong> If <code>\CoveoServer\Help\AdminTool\</code> is the main address and the <strong>Index subfolders</strong> check box is selected, then <code>\CoveoServer\Help\AdminTool\Sources\</code> and <code>\CoveoServer\Help\AdminTool\Sources\Local\</code> are also re-indexed or deleted.</td>
</tr>
<tr>
<td>Commit transaction after refreshing</td>
<td>All</td>
<td>Writes the transaction in the index at the end of the re-indexing or deleting process (see &quot;What Is a Transaction?&quot; on page 259).</td>
</tr>
</tbody>
</table>
The advanced parameters determine more precisely how a source is crawled, converted and indexed. The available advanced parameters vary according to the type of source.

To modify the advanced source parameters:

1. On the Coveo server, access the Administration Tool.
2. In the Administration Tool, select **Index > Sources and Collections**.
3. In the **Sources and Collections** page:
   a. In the Collections section, select the collection the source that you want to modify.
   b. In the Sources section, select the source that you want to modify.
   c. In the navigation panel on the left, select **Advanced**.
4. In the Advanced page, refer to the following table to configure the available advanced source parameters, and then click **Apply Changes**.

<table>
<thead>
<tr>
<th>Option</th>
<th>Applies to</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Add an exclusion filter</td>
<td>Remove from Index</td>
<td>Adds exclusion filters to keep Coveo Enterprise Search (CES) from re-indexing deleted documents during the next rebuilding or refreshing process (see &quot;Adding or Modifying Source Filters&quot; on page 295).</td>
</tr>
</tbody>
</table>

**c.** Click **Apply Changes**.

8.6.4.6.20 Modifying Advanced Source Parameters
<table>
<thead>
<tr>
<th>Section</th>
<th>Applies to</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Crawling</td>
<td>All sources</td>
<td>Determines which elements of a source are indexed (see &quot;What is the Structure of SharePoint?&quot; on page 513).</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Index hidden lists and their items</strong>: Indexes SharePoint hidden lists. Note that this option, which applies to SharePoint Legacy sources, is not selected by default.</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Index redundant issue list items</strong>: Indexes duplicate SharePoint Issues items. Note that this option, which applies to SharePoint Legacy sources, is not selected by default.</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Index survey responses</strong>: Indexes the responses to SharePoint Surveys. Note that this option, which applies to SharePoint Legacy sources, is not selected by default.</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Index documents uploaded with WebDAV</strong>: Indexes elements uploaded in SharePoint using WebDAV (i.e., elements invisible in the interface). Note that this option, which applies to SharePoint Legacy sources, is selected by default.</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Restrict crawling to X levels</strong>: Limits the crawling depth. This option applies to all sources and is not selected by default.</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Example: Restrict crawling to 2 levels</strong> indexes only the main address (\CoveoServer\Help\AdminTool) and addresses directly related to it (\CoveoServer\Help\AdminTool\Sources), other subfolders or subites (\CoveoServer\Help\AdminTool\Sources\Local) are not indexed.</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Allow crawling of external links</strong>: Indexes external Web pages directly linked to a website (but not their subpages). Note that this option, which applies to Web Pages sources, is not selected by default.</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Example: If</strong> <a href="http://www.coveo.com">http://www.coveo.com</a> contains a link toward <a href="http://microsoft.com">http://microsoft.com</a>, <strong>this latter page is indexed; however, <a href="http://www.microsoft.com/Careers">http://www.microsoft.com/Careers</a> is not.</strong></td>
</tr>
<tr>
<td>Section</td>
<td>Applies to</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------</td>
<td>--------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Disable cookies</strong>: Rejects cookies. This option is used when cookies keep the Coveo Platform from crawling a site (ex.: they redirect the connector elsewhere). Note that this option, which applies to <strong>Web Pages</strong> and <strong>SharePoint Legacy</strong> sources, is not selected by default.</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Expand sites and lists before applying filters</strong>: Builds the tree of SharePoint sites and lists before applying filters. This option allows the indexing of non-excluded children of excluded parent items. Note that this option, which applies to <strong>SharePoint Legacy</strong> sources, is not selected by default.</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Use the author extracted from the document instead of the SharePoint author</strong>: Extracts the authors of SharePoint documents using a conversion script. If this option is not selected, the metadata author name is used instead. Note that this option, which applies to <strong>SharePoint Legacy</strong> sources, is not selected by default.</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Use UTF-8 addresses</strong>: Indicates that the addresses of the documents are in UTF-8 instead of ANSI format. Note that this option, which applies to <strong>Web Pages</strong> sources, is not selected by default (see &quot;What Is the Difference Between ANSI and UTF-8 URI Formats?&quot; on page 311).</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Preserve file last access date</strong>: Preserves the last access date of the file—after indexing the file, the date is set to the last access date. When a user executes backups, it is important for the date of the file not to change if the file has not been accessed.</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Support robot exclusions</strong>: Indicates which robot exclusion rules (i.e. commands forbidding the crawling of a site) are respected by the Web connector. By default, all such rules are respected. However, it is possible to respect only <strong>Robots.txt</strong> or <strong>HTML META Tags</strong>. Moreover, it is possible to disregard all exclusion rules. Note that this option applies to <strong>Web Pages</strong> sources.</td>
</tr>
<tr>
<td>Download</td>
<td>Web Pages</td>
<td><strong>Timeout</strong>: Determines the number of seconds after which the Web connector disconnects from a source which is not responding. Note that the value entered in this field must be at least 1.</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Delay Between Downloads</strong>: Determines the number of seconds elapsed between each download made by the Web connector (pausing between downloads allows the site not to be queried continuously. A 10 second delay is the standard for Web connectors on the Web). Note that the value entered in this field must be comprised between 0 and 60.</td>
</tr>
<tr>
<td>Server Name Alias</td>
<td>Local/Network Files</td>
<td>Indicates the name of the server used to retrieve documents during queries - if it is different from the server crawled during indexing.</td>
</tr>
<tr>
<td></td>
<td>Web Pages</td>
<td><strong>Example</strong>: It is possible to index documents on a staging computer but open them from a production one. In this case, the name of the production server must be entered in the <strong>Server Name Alias</strong> box.</td>
</tr>
<tr>
<td></td>
<td>SharePoint Legacy</td>
<td></td>
</tr>
<tr>
<td>Tip</td>
<td></td>
<td><strong>Tip</strong>: The second generation SharePoint connector does not have this option, but uses a mapping file which allows you to override the Clickable and Printable URIs (see &quot;Creating and Using a Custom SharePoint Mapping File&quot; on page 1290). You need to create a metadata containing only the path part (i.e. no scheme and no server) of the original document URI to be able to replace it with a server alias.</td>
</tr>
<tr>
<td>Priority</td>
<td>All sources</td>
<td><strong>Priority</strong>: Determines the order in which sources are indexed - sources with <strong>Highest</strong> priority are indexed first; whereas, sources with <strong>Lowest</strong> priority are indexed last. Note that if sufficient memory and CPU resources are available, all sources can be indexed simultaneously.</td>
</tr>
</tbody>
</table>
### Section Table

<table>
<thead>
<tr>
<th>Section</th>
<th>Applies to</th>
<th>Description</th>
</tr>
</thead>
</table>
| Performance | All sources | Determines whether additional analysis of the document content is performed during the indexing process or not.  
**Disable advanced text layout analysis for PDF documents:** Disables the advanced analysis of PDF documents in order to save CPU resources and speed up indexing. The purpose of this advanced analysis is to improve ranking and summarization by determining the reading order of columns in PDF documents (ranking and summarization are affected by the order and proximity of words). Note that advanced analysis of PDF documents is enabled by default.  
**Disable advanced duplicate document filtering:** Disables the filtering of duplicate documents in order to save CPU resources and speed up indexing. The purpose of this advanced filtering is to display only one copy of each document in the result list. Note that the filtering of duplicate documents is enabled by default. |
| Conversion Timeout | All sources | Determines the number of minutes after which the converter proceeds to another document even if the conversion is not complete (the document for which the conversion has not been finished is considered corrupted). By default, the conversion timeout is of 10 minutes. |

### 8.6.4.6.21 What Are Wildcards?

Wildcards are symbols replacing a single character ( ?) or a string of characters ( *). They can be used in the search box but also in the Administration Tool to provide address patterns.

**Example:** `http://www.coveo.com*` represents all the pages of the Coveo website.

### 8.6.4.6.22 About Incremental Refresh and Live Monitoring

*Incremental refresh* and *live monitoring* are efficient processes which allow connectors to continuously keep the index up-to-date with new, modified, or deleted documents in a source.

Most Coveo connectors support either of these features. A connector will not support incremental refresh or live monitoring when the API of the repository type does not provide calls that allow the implementation of these feature or when the connector is in a prototype or beta state.

**Note:** You must manually enable incremental refresh for each source (see "Scheduling a Source Incremental Refresh" on page 433) while live monitoring is activated by default when supported, but can be turned off manually (see "Toggling Live Monitoring for a Source" on page 282).

### Incremental refresh

An incremental refresh makes the connector communicate with the repository at short intervals (ex.: every 5 minutes) to get new, modified, or deleted documents since the last incremental refresh run. With incremental refresh, source content changes must be pulled by the connector. Incremental refresh is supported by most connectors.

**Note:** In Coveo Platform versions prior to version 7, incremental refresh was named live indexing.
Live monitoring

Live monitoring registers repository events and immediately re-indexes new, modified, or deleted documents. With live monitoring, the connector listens to repository events. Source content changes are pushed to the connector by the repository. Live monitoring is however possible only with the "File Connector" on page 938 and the Sitecore Connector, which requires it to monitor RabbitMQ (see Administering RabbitMQ - On-Premises).

Notes:

- Because live monitoring is dependent of events registered by the Microsoft Windows file system, it is possible that some modifications are overlooked, especially when numerous events occur at the same time (live monitoring can handle approximately 4,000 events per minute). For file sources, it is therefore recommended to keep a source refresh schedule (see "Scheduling Source Refresh Actions" on page 435).

- Live monitoring cannot be enabled on a source whose address is a specific file (ex.: \\CoveoServer\HelpFiles\CESOnlineHelp.docx).

8.6.4.6.23 Limiting the Crawling Depth

The term crawling depth refers to the number of levels and sublevels of a repository indexed by the Coveo Platform. By default, CES indexes the starting address of a source and all its subfolders or subsites. However, it is possible to index only main folders or sites. Furthermore, it is possible to limit the depth or crawling by level.

Example: Restricting the depth of crawling to 2 levels indexes only the main address (\\CoveoServer\Help\AdminTool\) and addresses directly related to it (\\CoveoServer\Help\AdminTool\Sources\), other subfolders or subsites (\\CoveoServer\Help\AdminTool\Sources\Local\) are not indexed.

8.6.4.6.23.1 Indexing only the main folders or sites

1. On the Coveo server, access the Administration Tool.

2. In the Administration Tool, select Index > Sources and Collections.

3. In the Sources and Collections page, in the Sources section, expand the drop-down list of the source that you want to modify, and then select Edit General Properties.
4. In the **General** page:
   
a. In the **Options** section, clear the **Recursive** check box.

   b. Click **Apply Changes**.

8.6.4.6.23.2 Limiting the crawling depth by level

1. On the Coveo server, access the Administration Tool.

2. In the Administration Tool, select **Index > Sources and Collections**.

3. In the **Sources and Collections** page, in the **Sources** section, expand the drop-down list of the source that you want to modify, and then select **Edit Advanced**.
In the Advanced page:

a. In the Crawling section, select the Restrict crawling to X levels check box, and enter the appropriate number of levels.

b. Click Apply Changes.

8.6.4.6.24 What Is the Difference Between ANSI and UTF-8 URI Formats?

ANSI and UTF-8 are both encoding formats. ANSI is the common one byte format used to encode Latin alphabet; whereas, UTF-8 is a Unicode format of variable length (from 1 to 4 bytes) which can encode all possible characters.

By default, the Web Pages connector expects that addresses are in the ANSI format, but you can select the Use UTF-8 addresses option for a given source (see “Modifying Advanced Source Parameters” on page 305).

Note: When the Web Pages or the SharePoint connectors download web content, they expect documents with addresses encoded in UTF-8.

8.6.4.6.25 Manually Indexing Sources

Before performing a query in the search interface, the index must be populated; therefore, the sources configured must be crawled. Because this process requires considerable CPU resources, this operation is scheduled to be automatically executed at 12 AM.

You can however index one or more sources manually at any time.
To manually index sources

1. On the Coveo server, access the Administration Tool.

2. In the Administration Tool, select **Index > Sources and Collections**.

3. In the **Sources and Collections** page:

   - To index all the sources of a collection, in the **Collections** section:
     
     a. Select the check box for one or more collections that you want to index.
     
     b. In the **More Actions** drop-down list, select **Rebuild**.

   - To index specific sources of a collection, in the **Collections** section, click the collection, and in the **Sources** section:
     
     a. Select the check box for one or more sources that you want to index.
     
     b. In the **More Actions** drop-down list, select **Rebuild**.

8.6.4.7 Administration Tool - Top Results Menu

Top results are documents, corresponding to a query expression, which override the ranking process and are displayed before other search results.
You can identify Top Results with a star symbol (⭐) in the .NET search interface results. This option is not selected by default (see "Activating Search Interface Options With the .NET Interface Editor" on page 565).

**Example:** If the query Coveo Questions is frequently used to search Coveo Support FAQs, you can add this document as a Top Result (see "Adding Top Results to a CES Index" on page 313). Doing so displays the FAQs before other results when Coveo Questions is queried.

**Notes:**
- You can identify frequently queried expressions and their related documents (see "What Information Is Displayed in the Query Log?" on page 395).
- The JavaScript search does not support the Top Results, but with a Coveo Cloud index, you can use the equivalent Featured Results query pipeline feature (see Managing Query Pipeline Featured Results).

### 8.6.4.7.1 Adding Top Results to a CES Index

As a Coveo administrator, you can create Top Results for specific queries to ensure that important documents or items appear at the top of the search results when users perform those specific queries.

The Top Results feature is useful when someone in your organization wants to increase the visibility of a document in .NET search interfaces. You can identify frequent queries to which the document is related and create a Top Result for this document for each of the queries.

You can also use the Usage Analytics module (see "On-Premises Usage Analytics Module" on page 649) or the query log (see "What Information Is Displayed in the Query Log?" on page 395) to identify frequent queries for which the searched documents do not rank as high as they should, and create Top Results for these documents.

**Notes:**
- As a Coveo administrator, you can choose to show or not show the Top Result icon ⭐ next to the Top Result title/subject. This is done for each .NET Interface Editor using the Display top results icon option in the Interface Editor (see "Activating Search Interface Options With the .NET Interface Editor" on page 565).
- The JavaScript search does not support to show the Top Results icon ⭐ next to the Top Result title/subject.
- With Coveo Cloud, it is recommended to use the Featured Results query pipeline feature rather than index-level Top Results (see Managing Query Pipeline Featured Results).

You can create Top Results from the following Administration Tool pages:

- **Index Browser**
  
  The easiest method as you can select the document using the Index Browser search interface and apply the Add Top Result(s) action (see "Adding Top Results from the Index Browser" on page 314).

- **Top Results**
  
  The more formal method where you must type the document address, but allows you to set a Top Results for more than one document at a time (see "Adding Top Results from the Top Results page" on page 314).
8.6.4.7.1.1 Adding Top Results from the Index Browser

1. On the Coveo server, access the Administration Tool.

2. In the Administration Tool, select Content > Index Browser.

3. Using the Index Browser search interface, locate the document for which you want to create a Top Result, and then select Actions > Add Top Result (see "Finding Documents Using the Index Browser" on page 374).

   **Example:** Add the document Modularization of XHTML as a Top Result.

4. In the Add Top Result dialog box, enter one or more search queries for which you want this document to appear at the top of the result list, and then click OK.

8.6.4.7.1.2 Adding Top Results from the Top Results page

1. On the Coveo server, access the Administration Tool.

2. Select Index > Top Results.

3. In the Top Results page, click Add.

4. In the Add Top Results page:
a. In the **Queries** box, on separate lines, enter one or more query expressions for which you want to return a Top Result.

b. Click **Add Top Result**.

The **Collection**, **Source** and **Address** boxes appear.

c. In the **Collection** drop-down list, select the collection where the document to promote as a Top Result resides.

d. In the **Source** drop-down list, select the source where the document to promote as a Top Result resides.

e. In the **Address** box, enter the path of the document to promote as a Top Result. You can get this path from the Index Browser on the **Properties** line for the specific document (see "Reviewing Document Details from the Index Browser" on page 375).

**Notes:**

- In some cases, the Top Result may not work most likely because the path visible in the Index Browser and the path stored into the index are different. In these cases, rather use the Index Browser to create the Top Result (see "Adding Top Results from the Index Browser" on page 314).

  **CES 7.0.7711+ (June 2015)** Support for document URIs ending with a trailing wildcard (e.g., *).

  In this case, the Top Result is the first document that mostly matches the entered URI when documents are sorted alphabetically. This feature is useful for Sitecore setups where only the end of the document URI changes when the associated document does so.

f. To add another Top Result document for the same set of queries, click **Add Top Result**.

g. When you enter more than one Top Result document for a given set of queries, click the arrows (↑ and ↓) to set the order in which they are displayed in the .NET Interface Editor.

h. Click **Save**.
8.6.4.7.2 Managing Top Results in a CES Index

You can modify, disable/enable, or delete existing Top Results that are defined in your CES index.

To manage Top Results

1. On the Coveo server, access the Administration Tool.
2. In the Administration Tool, select **Index > Top Results**.
3. In the **Top Results** page:

   a. To modify an existing Top Result, click the Top Result that you want to modify, and in the **Top Result** page that appears:

   i. In the **Queries** box, on separate lines, you can add, delete or modify the query expressions for which you want to return the Top Result.

   ii. Click **Add Top Result** when you want to add documents to be promoted at the top of the results list when the specified queries are used.

   iii. Using the **Collection**, **Source** and **Address** boxes, select a new, or modify an existing Top Result
iv. Click **Apply Changes**.

b. To disable an active Top Result without deleting it, click **[Disable]** at the end of the corresponding Top Result line.

c. To reactivate a disabled Top Result, click **[Enable]** at the end of the corresponding Top Result line.

d. To delete a Top Result definition:
   i. Select the check box for the Top Result definition that you want to delete.
   ii. On the toolbar, click **Delete**.
   iii. At the confirmation message, click **Yes**.

8.6.4.8 Administration Tool - Ranking Menu

The **Ranking** menu section is useful to know how to fine-tune some of the pre-tuned ranking factors to better suit the needs of your organization.

8.6.4.8.1 Best Practices for Ranking Optimization

Ranking is the art of sorting results according to their relevance to the submitted query. Although CES is optimized to reach high ranking accuracy, improvements can still be realized by the content manager of the organization as each organization has its own set of rules and practices related to the document production and knowledge sharing.

You can optimize the ranking of results returned by CES using a few CES features. Document authors and people responsible for archiving documents can also adjust their document management process to improve document ranking.

Ranking optimization using CES features

- **CES ranking parameters**

  CES allows you to fine-tune ranking parameters according to specific needs or requirements of your organization (see "Customizing Search Results Ranking" on page 321).

- **Multiple sources**

  In CES, you can set a ranking score to each source according to the general estimated relevance of the documents contained in the source. Rating a source above others will favor documents found in this source.

**Example:** The source for the content in a legacy content management system (CMS) might be set with a lower ranking score compared to a source for a similar content in the new CMS.

As much as possible, divide your content in multiple sources instead of in one large source. This way you can set the rating separately for each source and refine the ranking.

**Example:** When indexing a network file server containing folders for each department, rather than creating one source for the whole file server, create one source for each department folder.
• **Top results**

Some frequent badly formulated queries may be bound to fail whatever ranking tuning process is applied. A CES mechanism named *Top Results* may help overcome this problem (see "Adding Top Results to a CES Index" on page 313). This feature allows to set a specific document or item to appear at the top or the results for one or a set of queries. The rest of the search results list is ranked normally.

• **Query Ranking Expressions**

You can add query ranking expressions (QRE) to a search interface to adjust the search results ranking only for this interface (see "What Are Query Ranking Expressions?" on page 612).

**Ranking optimization adjusting document management process**

• **File and folder naming conventions**

Some of the ranking parameters are related to the document path. This path is made of the concatenation of several folder names and one filename. Thus, to ensure ranking accuracy, choose suitable and meaningful names for folders and files. A simple and easy method to clarify names is to insert separating characters between words within file and folder names.

**Example:** The query `super` would not be matched against `c:\Superaudio\docs` but it would against `c:\Super_audio\docs` or `c:\Super audio\docs`.

Whenever possible, in the path or filename, use both the acronym and its corresponding meaning, such as `c:\companies\Super car audio - SCA\docs`. As a result, both the `query Super car audio` and `SCA` match this path.

• **Organizational vocabulary and metadata**

There are often equivalences among the terms used by people within an organization.

**Example:** The acronym `SCA` might be used instead of `Super car audio`. Nonetheless, the `query SCA` would not match any document that only contain `Super car audio` and never mention the acronym `SCA`.

To remedy this problem, metadata content can be created to be indexed when such interchangeabilities occur. Many document formats (HTML, PDF, Word…) provide methods to include metadata. Refer to the documentation of the software used to create the various file formats to include appropriate metadata and set appropriate values.

**Example:** An HTML file that contains `SCA` in the body text can have a `META KEYWORDS` set to `Super car audio`.

• **Document titles**

The users naturally search for a document expecting to find a specific document title. Authors of documents must choose short and accurate titles. CES uses the document title separately from the rest of the content in the ranking process. In the title score calculation, the proportion of the title that matches the query is taken into account.
**Example:** For the query **Order Form**, a document entitled **Super Car Audio – SCA Car Audio – International Order Form Access Page** would get less title points than a document entitled **International Order Form**, since a larger part of the title of the latter document matches the query.

Authors must also properly set the title in the properties of each file format. When no title metadata exists in a document, CES guesses that the first sentence is the title. With a proper title property, a query specifically searching for a given document title is almost guaranteed to return the right result in the first positions.

**Example:** In Microsoft Word, the title must be entered in the **Title** field in document properties.

### 8.6.4.8.2 What Is Collaborative Rating?

Collaborative rating is a ranking factor based on personal appreciation (star rating) and the number of clicks on each document. It calculates an average of the appreciations given to each document by users of the same group and takes in account the click count on each document, and uses this average and click-through rate to fine-tune ranking. Because this process is performed independently for each user group, it tailors ranking to different types of users.

However, calculating this factor requires considerable CPU resources and can slow down CES. If this problem occurs, apply the rating to fewer documents (ex.: the 50 top ranking documents) (see "Customizing Search Results Ranking" on page 321).

Collaborative rating is displayed as a number of grey stars under each document (☆☆☆); whereas personal appreciation is displayed as a number of yellow stars (☆☆☆). Personal appreciation prevails on collaborative rating meaning that, once a document is rated by a user, its collaborative rating score is no longer taken into account during the ranking process.

**Note:** Collaborative rating is optional and must be managed independently for each search interface:

- For .NET search interfaces (see "Activating Search Interface Options With the .NET Interface Editor" on page 565 and "Configuring Collaborative Rating" on page 319).
- For JavaScript search interfaces (see Enabling and Adding Collaborative Rating to a JavaScript Search Page).

### 8.6.4.8.3 Configuring Collaborative Rating

You can activate or disable collaborative rating, set on the number of best documents it applies, and specify users or groups that can use it.

To configure collaborative rating

1. On the Coveo server, access the Administration Tool.
2. In the Administration Tool, select **Index > Ranking**.
3. In the panel on the left, select **Collaborative Rating**.
4. In the **Collaborative Rating** page:
To disable the collaborative rating feature, in the Status section, click [Disable].

You will be prompted to confirm this action as it will delete all the personal appreciations entered so far by users. To re-enable the feature, click [Enable] that appears at the end of the Status section.

In the Option section, you can change the number of top ranking documents on which collaborative rating is available. The default value is 100, meaning that users can set a personal appreciation only on the first 100 top ranking search results documents.

**Note:** This value is configurable from 10 to 10,000.

In the Valid Groups list, you can control with who users share their ratings by specifying groups. By default, every user shares their ratings with every member of every group.

**Note:** Users that are member of one or more groups in the Valid Groups list share their ratings with the other members of the same groups.

**Example:** In your organization, you want members from your marketing department to only share their ratings with the members of their group so you add the marketing group in the Valid Groups list. If members of your marketing group are also members of other Valid groups, their ratings will also be shared with the other groups.

  i. To remove a valid group, select it in the Valid Groups list, and then click Remove.

  ii. To add a group, click Add, and then in the Add Identity dialog box, select the group for which you want the members to only share their ratings between them (see "Using the Identity Picker Form" on page 428).

  d. Click Apply Changes to save your changes.
8.6.4.8.4 Customizing Search Results Ranking

CES uses 15 ranking factors divided into 6 types to calculate the relevance score of documents. CES natively uses pre-tuned ranking weights that are likely to be satisfying most of the time. Nevertheless, fine-tuning these factors can sometimes increase accuracy, especially for specific situations.

**Example:** An organization may find not important that a recent document modification date contribute to a higher rank.

As a Coveo administrator, you can fine-tune the ranking of search results by adjusting the weight of each ranking factor and specify ignored fields, fields whose values are not taken into consideration when ranking results. By default, each of these factors is assigned a weight of 5 on a scale of 1 to 9, where 9 corresponds to the highest ranking weight.

To customize the weight of ranking factors

1. On the Coveo server, access the Administration Tool.
2. In the Administration Tool, select **Index > Ranking**.
3. In the navigation panel on the left, select **Ranking Weights**.
4. In the **Ranking Weights** page:
a. For each factor:

- Select a higher value to increase the importance of a factor.
- Select a lower value to decrease the importance of a factor.
- Select **Ignore** to exclude a ranking factor from the ranking process.

**Note:** Even if all factors have the same weight (ex.: 5), their relative importance is not necessarily identical as CES uses a built-in weight for each factor. For example, **Term in title** has more effect on the final ranking than **Document modified recently**.

Each ranking factor value is relative to the other factor weights. The resulting ranking is the same whether all multipliers are set to 4 or if they are all set to 2. You can give a higher weight to a factor by setting it to 7 and all others to, for example, 2. The relative weight of 7 against 2 is much higher than 7 against 4.

Refer to the table that follows for details on each ranking factors.
<table>
<thead>
<tr>
<th>Type</th>
<th>Factor</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Content</td>
<td>Term frequency</td>
<td>Higher relevance score to documents in which query terms are frequently repeated. The importance increases proportionally to the number of times a query term appears in a document relative to the number of times it appears in the index.</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Example:</strong> A document in which a term is repeated 10 times receives a higher ranking than one of the same size in which it is repeated only 2 times.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>The frequency factor has a higher ranking impact when searching for a term such as <em>suspicious</em> that probably occurs rarely in an index, compared to a term such as <em>the</em> that most likely occurs a large number of times in the index.</td>
</tr>
<tr>
<td></td>
<td>Term proximity</td>
<td>Higher relevance score to documents in which query terms are close to each other. This factor applies only when the query contains more than one term.</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Example:</strong> A document in which the terms are only one word apart receives a higher ranking than one in which they are ten words apart.</td>
</tr>
<tr>
<td></td>
<td>Term in title</td>
<td>Higher relevance score to documents containing query terms in their titles. Moreover, relevance is dependent on the proportion of title terms matching the query.</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Example:</strong> If the query term is <em>Coveo</em>, a document with the title <em>Coveo Enterprise Search</em> (one out of three words matches the query) receives a higher ranking than one with the title <em>Enterprise Search</em>, or <em>Coveo Enterprise Search Provides Businesses with the Most Collaborative and Agile Search Solution Available</em> (one out of 14 words matches the query).</td>
</tr>
<tr>
<td>Type</td>
<td>Factor</td>
<td>Description</td>
</tr>
<tr>
<td>----------------------</td>
<td>---------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Term in concepts</td>
<td>Higher relevance score to documents containing query terms in their lists of concepts. Concepts are extracted by the CES linguistic algorithm which relies on term frequency and proximity.</td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong> If the query is Coveo, a document for which the concept Coveo has been extracted receives a higher ranking than one for which this concept has not been extracted (even if the word Coveo is present in its content).</td>
<td></td>
</tr>
<tr>
<td>Term in summary</td>
<td>Higher relevance score to documents containing query terms in their summaries. Summaries are extracted by the CES linguistic algorithm which relies on term frequency and proximity.</td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong> If the query term is Coveo, a document for which the key topic Coveo has been extracted in its summary receives a higher ranking than one for which it has not been extracted (even if the word Coveo is present in its content).</td>
<td></td>
</tr>
<tr>
<td>Term correlation within stemming classes</td>
<td>Higher relevance score to documents words with the same root as the query terms and that are often found co-occurring in indexed documents.</td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong> If the query term is universal, a document containing the word universality receives a higher ranking than one containing university when universal and universality have a higher co-occurrence rate than universal and university in indexed documents.</td>
<td></td>
</tr>
<tr>
<td>Document</td>
<td>Documents modified recently</td>
<td>Higher relevance score to documents whose modification date is recent.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong> A document modified today receives a higher ranking than one modified a month ago.</td>
<td></td>
</tr>
<tr>
<td>Document quality evaluation</td>
<td>Higher relevance score to documents which are close to the root of a file system.</td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong> A document located in C:\Docs\ receives a higher ranking than one located in C:\Docs\Projects\Project\Planning.</td>
<td></td>
</tr>
<tr>
<td>Document in user language</td>
<td>Higher relevance score to documents in the same language as the search interface.</td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong> If the search interface is in English, a document written in English receives a higher ranking than one written in French.</td>
<td></td>
</tr>
<tr>
<td>Location</td>
<td>Source rating</td>
<td>Higher relevance score to documents contained in a source rated Highest to Above Normal as you can individually set the rating of each source (see “Adding a Source” on page 281).</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong> If the query term is Coveo, a document whose address is <a href="http://www.coveo.com/en/Support/Default.aspx">http://www.coveo.com/en/Support/Default.aspx</a> receives a higher ranking than one whose address is <a href="http://support.microsoft.com/">http://support.microsoft.com/</a>.</td>
<td></td>
</tr>
<tr>
<td>Type</td>
<td>Factor</td>
<td>Description</td>
</tr>
<tr>
<td>--------------</td>
<td>---------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
</tbody>
</table>
| Formatting   | Term has formatting             | Higher relevance score to documents containing query terms in large fonts or bold.  
**Example:** If the query term is Coveo, a document containing the word *Coveo* receives a higher ranking than one containing the word *Coveo*. |
|              | Term casing                     | Higher relevance score to documents containing the same casing as the query term.  
**Example:** If the query term is *iPad*, a document containing the word *iPad* receives a higher ranking than one containing the word *Ipad*. |
| Collaborative| Collaborative rating weight     | Higher relevance score to documents whose collaborative rating score is high (see "What Is Collaborative Rating?" on page 319) when users voice their personal appreciation of documents.  
**Note:** Collaborative rating must be enabled for this factor to apply but it is by default. Calculating collaborative ratings may require considerable CPU resources and can slow down CES. If this problem occurs, consider reducing the number of top documents to which it applies (ex.: 50), reducing the number of groups or simply disabling collaborative rating (see "Configuring Collaborative Rating" on page 319). |
| Custom       | Custom ranking weight           | Determines the importance that must be given to documents whose custom ranking weight has been set. Custom ranking factors are scripted directly in open converters (see "Administration Tool - Converters Menu" on page 455 and "Adding a Connector" on page 444). |

b. In the **Ignored Fields** box that already contains built-in fields that should be excluded, add the custom fields that you want to exclude from the ranking results (see "What is the Difference between Built-In and Custom Fields?" on page 490).  
**Example:** If the query expression is Coveo AND @syslanguage=English, occurrences of the term *English* do not affect ranking because *syslanguage* is an ignored field. However, if *syslanguage* is removed from the **Ignored Fields** list, ranking is adversely affected because documents containing occurrences of the word *English* receive a higher ranking. Whereas, the purpose of *syslanguage* is to find documents written in English, not to display all documents with the word *English* in them. If custom fields can have a similar effect on ranking, add them to the **Ignored Fields** list.

c. Click **Reset** below the label of a factor category, to return the weight of ranking factors for that category to their default value of 5.

d. Click **Apply Changes** to save your modifications.

e. Ensure your modifications improve search result relevance by looking at the detailed ranking information in your search interface(s) ("Troubleshooting Ranking" on page 329).
8.6.4.8.5 Index Ranking Phases

The CES ranking engine is the component responsible for the ordering of query results. Basically, it makes sure the most relevant results are shown before less relevant ones based on your settings.

This mechanism behind the ranking process can be compared to a funnel. Starting with all documents, the index receives a query from a user, isolates documents in which the user identity can be found in the permission groups (see Security Control Levels in CES and Document Permissions), and then only keeps the documents that match the query.

The ranking process is separated into five phases, each of them working on the documents sorted by the preceding phase.

CES natively uses 16 pre-tuned ranking weight factors during these phases. For example, among the most important ones, the criteria with the biggest relevance impact are term proximity, document modified date (most recent), and term frequency. Each of these 16 criteria has been optimized over years of experience with a wide variety of indexed content to determine highly satisfying out-of-the-box relevance scores of documents in most cases. You can still carefully tune these parameters when needed (see "Customizing the Ranking for a .NET Search Interface" on page 613). You can also troubleshoot ranking when a factor score seems too high or too low (see "Troubleshooting Ranking" on page 329).

**Important:** While you can use several parameters to tune the index ranking engine, you must make changes carefully to prevent negative performance or ranking collateral effects. It is recommended to contact Coveo Support to get recommendations to address your index ranking issues.

<table>
<thead>
<tr>
<th>Phase</th>
<th>Ranking factor (UI label)</th>
<th>Applies to n best ranked documents from the previous phase</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Term in title (Title)</td>
<td>All matching security and query</td>
</tr>
<tr>
<td></td>
<td>Term in concepts (Concept)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Term in summary (Summary)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Terms in address (URI)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Term has formatting (Formatted)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Term casing (Casing)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Term correlation within stemming classes (Relation)</td>
<td></td>
</tr>
</tbody>
</table>
### Phase: Ranking factor (UI label) | Applies to n best ranked documents from the previous phase
---|---
| Documents modified recently (Date) | 50 000² |
| Document quality evaluation (Quality) |  |
| Document in user language (QRE) |  |
| Document title match (Title)¹ |  |
| Source rating (Source) |  |
| Custom ranking weight (Custom) |  |
| Collaborative rating weight (Collaborative Rating) | 100² |
| Term frequency (Frequency) | 100² |
| Term proximity (Adjacency) | 100² |

¹ Not configurable in the UI.
² Default value that is configurable.

**Note:** The relative importance of each of the ranking criteria is difficult to establish, since each criteria score depends on many factors, such as the number of terms in the query, the type of sources that are indexed, the individual terms in the query and the number of documents in the index.

#### 8.6.4.9 Phase 1: Term weighting

The first phase attributes a score to documents based on each term of the user query. Seven factors are used to rank the indexed documents the user has permissions to access and match the query. These factors cover areas such as the position of the query terms in those documents (in the title, in the summary, in the concepts, etc.). Once the ranking is done, the 50,000 highest scored documents are kept.

**CES 7.0.6339+ (January 2014)**, On top of these ranking factors, query ranking expressions (QRE), which are custom expressions used to modify the ranking score by a specified amount when documents match certain conditions, are taken into account during this phase (see "What Are Query Ranking Expressions?" on page 612).

**Notes:**

- A CES administrator can fine-tune the importance of each of the factors, but this should be done with care because it affects all results in all search interfaces (see "Customizing Search Results Ranking" on page 321).
- For each document, the score attributed for each factor is shown under **Term Weights** (see "Troubleshooting Ranking" on page 329).
8.6.4.10 Phase 2: Document weighting

The second phase attributes a score to documents based on their freshness (last modification date) and quality. This phase, which is performed on the first 50,000 documents with the highest ranking scores returned by phase one, uses six ranking factors that cover areas such as the document language (same language as the user query or not) and source rating (reputation from lowest to highest) to further adjust the relevance score of these 50,000 documents. Once the ranking is done, the 100 highest scored documents are kept and the next three index ranking phases are performed on these documents.

Notes:

- A CES administrator can fine-tune the importance of each of the factors, but this should be done with care because it affects all results in all search interfaces (see "Customizing Search Results Ranking" on page 321).
- A CES administrator can modify the rating of a source, and thus the rating of the documents it contains (see Modifying General Source Parameters).
- This phase involves loading document-specific information such as if the documents were modified recently.
- For each document, the score attributed for each factor is shown under Document Weights (see "Troubleshooting Ranking" on page 329).

8.6.4.11 Phase 3: Collaborate ranking

When collaborative rating is enabled, the third ranking phase attributes a score to documents by considering the average of the personal appreciations given to each of those documents by members of the same group of the user performing the query [if any] (see "What Is Collaborative Rating?" on page 319). This phase is performed on the 100 documents returned by phase two. Once the ranking is done, the documents are reordered from the highest scored at the top to the lowest scored at the end.

Notes:

- A CES administrator can enable collaborative rating (see "Configuring Collaborative Rating" on page 319).
- Personal appreciation prevails on collaborative rating meaning that, once a user rates a search result, the collaborative rating score of this document is no longer taken into account.
- For each document, the score attributed for Collaborative rating is shown under Document Weights (see "Troubleshooting Ranking" on page 329).

8.6.4.12 Phase 4: Term frequency–inverse document frequency (TF-IDF)

The purpose of the fourth phase is to weight queried terms while taking their number of occurrences in documents into account.

The ranking engine evaluates the importance of a query term for a document based on the number of occurrences of this term in the document, but also inversely on the number of occurrences of the term in the index (TF-IDF). The more frequent a term is in the index, the less informative the term becomes since the significance and meaning are to a certain extent diluted.
Example: A common term such as product is worth less than a rare one such as iPhone.

Based on this methodology, each of the 100 documents returned from phase three receives an additional score, and then their ranks are adjusted accordingly.

Notes:

- A CES administrator can modify the number of documents on which phase four applies in the Administration Tool using the Optimization parameter (see "Modifying or Using Advanced Index Parameters" on page 366).
- For each document, the score attributed for Frequency for each queried terms is shown under Term Weights (see "Troubleshooting Ranking" on page 329).

8.6.4.13 Phase 5: Adjacency ranking

The last phase computes the proximity of query terms, giving more weight to documents having the terms close together in the text. This step fine-tunes the order of the documents received from phase 4 and, once the reordering is done, documents are returned in the search interface to the user as a response to the submitted query.

Notes:

- Term proximity does not apply to queries with one term and is only calculated on a maximum of 100 documents. Contact Coveo Support to receive assistance on how to modify this value that can be 400, 300, 200, 150, or 100. If bigger than 400, the number is reduced to the one set in the Optimization box (see "Modifying or Using Advanced Index Parameters" on page 366).
- For each document, when ranking information is enabled, the score attributed for Adjacency is shown under Document Weights (see "Troubleshooting Ranking" on page 329).
- The value of the docID is used to break ties (if any) and ensure the same results order is respected if the same query is performed in the future. Documents with the same ranking score are sorted in descending docID values order.
- By default, ten results are shown per page in your search interface, meaning that past the tenth page, results were not processed by the last three phases.

This is how ranking is involved within relevancy. However, the ranking process is not limited to these phases. CES comes with many features that further help fulfill your needs. Features that you can use to personalize or customize the way you want your documents to be ranked. Top results, personal appreciation and ranking functions are among other factors influencing the relevance or search results.

8.6.4.13.1 Troubleshooting Ranking

When one or more queries do not return the results that you expect, you can use, among other things, the relevance score of problematic results to solve your ranking matters.

To troubleshoot ranking

1. In a Coveo search interface, in the search box, perform the following query:

   enablerankinginformation
This query adds document ranking weight information to the JavaScript search interface debug page or to the search result details in a Coveo .NET Front-End search interface.

**Note:** Because adding this information can have a performance impact, the feature is enabled only for your user.

2. Perform a query that needs to be troubleshooted.

3. Look at the detailed ranking information:

   - For Coveo .NET Front-End search:
     
     a. In a Coveo .NET Front-End interface, at the bottom of a search results, click **Details**.
        
        The Details section expands.
     
     b. In the Details section, click the **Ranking weights** tab.

   ![Example of Ranking weights tab](image)

   - For the Coveo JavaScript Search:
     
     a. In a Coveo JavaScript interface, press `Alt` + double-click the search result description.
        
        The **Debug** window appears.
     
     b. In the **Debug** window, scroll down to the **Ranking Info** section.

   ![Example of Ranking Info section](image)

   **Note:** The ranking weight of the result is next to **Total weight**, which is the sum of the **Document weighs** and **Terms weights**. The more weight a result has, the higher it appears in the results list. Each of these ranking factors can be customized as well as the number of results in each index ranking phases (see "Customizing Search Results Ranking" on page 321 and "Index Ranking Phases" on page 326).
4. Look for any numbers that contrast with the others and take action.

**Example:** You query for `sales tax` and the first search result that is returned does not satisfy you. You see that the result has a score of 1500 in **Adjacency** so you go in the **Ranking Weights** page and lower the ranking score for **Term proximity**.

### 8.6.4.14 Thesaurus Menu

The **Thesaurus** page is useful to add and review related or equivalent words used to expand queries by transparently adding expressions to the search, thus returning more results that would otherwise be missed.

### 8.6.4.14.1 Thesaurus Best Practices

When managing thesaurus entries (see "Adding Thesaurus Entries From the Administration Tool" on page 332), consider the following rules, behavior, recommendations, and tips:

- Matching acronyms and abbreviations with their full versions, or jargon with proper terminology is a good thesaurus usage.

- Taking advantage of either the on-premises or cloud usage analytics (see "On-Premises Usage Analytics Module" on page 649 or "Usage Analytics Cloud Service" on page 677), identify searched keywords that return no or not optimal results because users are not searching for the terms used in the available content, and then create a thesaurus entry that expands the query to the appropriate synonyms.

- A thesaurus entry is expanded for an exact match only (the stemming expansion is applied after the thesaurus expansion), so you should consider entering singular/plural, conjugation, one vs two-word, and other synonym variants to increase chances the entered keyword is expanded.

- Thesaurus entries are case insensitive, so do not bother entering casing variants.

- Avoid adding a large number of thesaurus entries without a precise search optimization goal (for example using an external glossary) to prevent adverse side effects that can confuse users.

- Avoid using the thesaurus to expand a typo to its correct form. Based on the relative occurrences of a misspelled and correct form of a word in the index, the query correction (or **Did You Mean**) feature will automatically suggest or correct the best spelling (see "Query Correction Feature" on page 273).

**Note:** The **Did You Mean** feature notifies users of the term suggestion/correction, while the thesaurus silently expands or replaces query terms. The thesaurus expanded or replaced terms are however highlighted in search result titles and excerpts, as are other queried terms.

- A specific keyword/expression can only appear once across thesaurus entries. You must group equivalent keywords/expressions in one thesaurus entry.

- Be careful to enter only legitimate synonyms to prevent excessive search result broadening that can negatively
affect search results ranking and confuse users.

- Minimize the number of synonyms that you enter in a given entry to prevent confusing the users with numerous matching terms and also prevent drastically increasing the length and complexity of the query.

  **Note:** All thesaurus expanded query keywords are stemmed and expanded to other shared-root keywords, further increasing the length of the query.

- The thesaurus applies only to free text queries, not to field queries.
- Thesaurus entries are not applied for keywords entered next to the NOT and NEAR operators.
- Immediately test your thesaurus entry creation or modification in the search interface(s) to ensure that they improve search result relevance.

### 8.6.4.14.2 Adding Thesaurus Entries From the Administration Tool

The CES thesaurus is a list of related or equivalent words used to expand queries. The thesaurus transparently adds expressions to the search, thus returning more results that would otherwise be missed. You can easily populate the thesaurus using the Administration Tool (see "Thesaurus Best Practices" on page 331).

**Example:** The thesaurus is useful to expand queries for abbreviations. When a user enters the short form of an expression like XML, the thesaurus adds to the query the long form of the expression like extensible markup language, thus returning results containing either form of the expression.

**Note:**

- You can also manually edit the XML file of the thesaurus (see "Creating or Modifying a Thesaurus XML File" on page 335).
- With a Coveo Cloud index and Coveo JavaScript Search interfaces, rather use the query pipeline Thesaurus feature (see Managing Query Pipeline Thesaurus).

To add a thesaurus entry

1. On the Coveo server, access the Administration Tool.
2. In the Administration Tool, select Index > Thesaurus.
3. In the navigation panel on the left, click Keywords.
4. In the right pane, click Add.
5. In the Add Thesaurus Keyword page:
a. In the **Keyword** box, enter the word or exact phrase for which you want to enter one or more synonyms.

   **Example:** To add *bob* to the query *robert*, enter *robert* as the keyword.

b. In the **Synonyms** box, enter one or more words to add as synonyms of the keyword. When entering more than one synonym, enter one entry per line. You can enter an exact phrase.

   **Example:** To add *bob* to the query *robert*, enter *bob* as the synonym.

   **Note:** You cannot use search prefixes or operators such as OR, AND, or NEAR to define **Keyword** and **Synonyms**.

c. In the **Option** section:

   - Clear the **Use the synonym relationship advanced rule** check box to use the basic relationship rule that adds the synonyms to the keyword using the OR operator.

   OR

   - Select the **Use the synonym relationship advanced rule**.

     i. Select **Replace the keyword by its synonym** to replace the keyword by the synonym. This synonymy rule allows only one synonym per keyword.

     **Note:** You cannot use the same keyword twice, meaning that a specific keyword can only be contained in one rule.
Example: A query for robert becomes bob.

OR

Select Establish reciprocal synonymy between the keyword and its synonyms to add the synonym to the keyword using the OR operator and vice versa.

Example: A query for robert becomes robert OR bob and a query for bob becomes bob OR robert.

Note: Selecting this option is equivalent as setting the attribute bidirectional=true for the mapping tag in the XML thesaurus file.

d. In the Collection box, you can select one or more collections that must be specifically selected for search in a .NET Interface Editor to allow the thesaurus entry expansion. By default, no collection is selected, meaning that the thesaurus entry is always expanded (for all collections), in any Coveo .NET Front-End search interface.

Important: The conditions required to make this feature work (explained in this step) are not obvious and often misunderstood, leading to thesaurus entries not taking effect. The easy solution to ensure a thesaurus entry takes effect is to clear all collection check boxes.

Note: A Coveo .NET Front-End search interface specifically selects one or more collections for search when its scope does not include all available collections. You can see and set the scope of a Coveo .NET Front-End search interface from the .NET Interface Editor in the Search Interfaces > Features > Scope page. In this page, for thesaurus entry collection restriction to work, under Available Collections, select one or more (but not all) collections, and under Scope Configuration, select No Scope (see "Configuring the Scope of a .NET Search Interface" on page 597).

Example: In the Administration Tool, you create a thesaurus entry for robert and bob, and only select the R&D collection.

In your Coveo .NET Front-End R&D Stuff search interface that includes the R&D collection in its scope, the query robert is expanded to bob.

In your Coveo .NET Front-End Human Resources search interface that does not include the R&D collection, the query robert is not expanded to bob.

In the default Coveo .NET Front-End All Content search interface, that by default includes all collections and does not specifically select collections for search, the query robert is not expanded to bob. However, if you use the Advanced Search page to select one or a few available Collections including the R&D collection, then the interface specifically selects these collections and the query robert is expanded to bob.

In the Administration Tool, when you select one, a few, or all available collections for a given thesaurus entry, the thesaurus entry is expanded when at least one of the selected collections are selected for search in a given .NET Interface Editor, and the thesaurus entry is expanded for all collections included in the scope of the .NET Interface Editor.
**Example:** Your index is made of 5 collections (A, B, C, D, E). You assign a thesaurus entry to collections A and B. In a Coveo .NET Front-End search interface with a scope that includes collections B, C, and D, the thesaurus entry is expanded for documents from collections B, C, and D.

**Important:** Currently, a Coveo JavaScript search interface cannot specifically select one or more collections for search. Consequently, a thesaurus entry for which you selected one or more collections will never be expanded in a Coveo JavaScript Search interface.

When your Coveo deployment includes only Coveo JavaScript Search interfaces (no Coveo .NET Front-End search interfaces), do not select collections. Rather use the thesaurus feature available from the REST Search API (see Thesaurus).

**Note:**
- **CES 7.0.7256– (December 2014)** Selecting all collection check boxes results in the thesaurus entry being applied for none of the collections. This issue was corrected in CES 7.0.7338 (January 2015 release).
- **CES 7.0.6607– (April 2014)** The **Collection** option is a drop-down list where you can select either **All Collection**, the default, or one specific collection.

6. Click **Save**.

8.6.4.14.3 Creating or Modifying a Thesaurus XML File

The CES thesaurus is a list of related or equivalent words used to expand queries. It works by transparently adding expressions to the search.

If you are familiar with the structure of XML documents, editing the corresponding file manually is an effective way to populate the thesaurus. You can also add synonyms using the Administration Tool (see "Adding Thesaurus Entries From the Administration Tool" on page 332).

**Important:** XML syntax errors disable the thesaurus file and display the following message in the Thesaurus page (Index > Thesaurus): **Object reference not set to an instance of an object.**

The following table describes the valid tags and attributes that a thesaurus XML file contains.

<table>
<thead>
<tr>
<th>Tag</th>
<th>Attribute</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>mappings</td>
<td></td>
<td>Starting/closing thesaurus file tag.</td>
</tr>
<tr>
<td>Tag</td>
<td>Attribute</td>
<td>Description</td>
</tr>
<tr>
<td>--------------</td>
<td>-----------</td>
<td>-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>mapping</td>
<td>keyword=</td>
<td>Identifies the keyword to which synonyms are added.</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Example:</strong> To add Coveo to the query CES, enter: <code>&lt;mapping keyword=&quot;CES&quot;&gt;</code>. Enter only one keyword attribute per mapping tag. You can however enter an expression (more than one word), in which case it is interpreted as an exact phrase, so the thesaurus entry is expanded only when users enter this exact phrase (same words in same order).</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Example:</strong> <code>&lt;mapping keyword=&quot;Coveo Enterprise Search&quot;&gt;</code>.</td>
</tr>
<tr>
<td></td>
<td>type=</td>
<td>Indicates the operator (or or replace) used to add synonyms to the query.</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Example:</strong> With robert being a synonym for bob, when you use or, a query for bob becomes bob OR robert. When you use replace, the same query becomes robert.</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Note:</strong> To use the replace operator, the keyword must have only one synonym. The replace operator is incompatible with the bidirectional=true attribute.</td>
</tr>
<tr>
<td></td>
<td>bidirectional=</td>
<td>Indicates whether the synonymy is reciprocal or not.</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Example:</strong> With robert being a synonym for bob, when you use true, a query for bob becomes bob OR robert and a query for robert becomes robert OR bob. When you use false, a query for robert remains robert.</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Note:</strong> The bidirectional=true attribute is incompatible with the type=replace attribute.</td>
</tr>
<tr>
<td>synonyms</td>
<td></td>
<td>Encloses all occurrences of synonym tags.</td>
</tr>
<tr>
<td>synonym</td>
<td>value=</td>
<td>Identifies the expression to add as a synonym of the keyword.</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Example:</strong> To add robert to the query bob, enter robert as synonym: <code>&lt;synonym value=&quot;robert&quot;/&gt;</code>. You can enter more than one synonym for a given keyword.</td>
</tr>
</tbody>
</table>

**Note:** You cannot use search prefixes or operators such as OR, AND, or NEAR to define keyword and synonym tag values.

Creating an XML thesaurus file

2. Start the thesaurus file content with the `<mappings>` opening tag.
3. Enter each keyword-synonym mapping in the format illustrated by the following example.

   ```xml
   <mapping keyword="bob" type="or" bidirectional="false">
     <synonyms>
       <synonym value="robert"/>
     </synonyms>
   </mapping>
   ```

4. Close the thesaurus with the `</mappings>` closing tag.
5. Save the file with a name of your choice and the xml extension. The recommended folder is [Index_
6. Import the new thesaurus file in CES to activate it (see "Importing a Thesaurus XML File in CES" on page 337).

Modifying an existing XML thesaurus file:

1. Using a text editor, open the existing thesaurus file.

Example: C:\CES7\Config\DefaultThesaurus.xml

2. Enter each keyword-synonym mapping in the following format.

   \[<mapping keyword="bob" type="or" bidirectional="false">
   <synonyms>
   <synonym value="robert"/>
   </synonyms>
   </mapping>\]

3. Save the file.
4. Refresh the thesaurus (see "Refreshing the Thesaurus" on page 338).

8.6.4.14.4 Importing a Thesaurus XML File in CES

Once a custom thesaurus file has been created, you need to import it in CES to activate its content for query expansion.

To import a thesaurus file

1. On the Coveo server, access the Administration Tool.
2. In the Administration Tool, select Index > Thesaurus.
3. In the Thesaurus page:

   a. In the navigation panel on the left, click General.
   b. In the Thesaurus XML File box, enter the path of the new thesaurus file.
The recommended folder is [Index_Path]\Config.

Example: D:\CES7\Config\MyThesaurus.xml

c. In the Option section, select the Apply thesaurus to field queries check box when you want the thesaurus entries to also expand field queries.

Note: By default, the thesaurus applies only to free text queries. In general, it does not make sense to apply the thesaurus to field queries because the purpose of field queries is to refine searches; whereas, the purpose of the thesaurus is to expand them. You may however encounter situations where it is desirable to also apply the thesaurus to field queries.

d. Click Apply Changes.

The thesaurus is loaded when the CES service starts.

4. You can refresh the thesaurus file without restarting the service (see "Refreshing the Thesaurus" on page 338).

8.6.4.14.5 Refreshing the Thesaurus

The thesaurus is loaded when the CES service starts. To apply subsequent modifications, you can load the thesaurus manually to avoid having to restart the CES service.

To refresh the thesaurus

1. On the Coveo server, access the Administration Tool.
2. In the Administration Tool, select Index > Thesaurus.
3. In the Thesaurus page:
   a. In the navigation panel on the left, click General.
   b. Click Refresh Thesaurus.

8.6.4.15 Administration Tool - Mirrors Menu

The Mirrors page allows you to manage the Mirror servers and slices of the index.

8.6.4.15.1 Adding a Mirror Server

A Mirror server hosts a copy of the original index from the Master server (see "About Mirror Servers" on page 18). After commissioning a server and installing a Mirror server software, you must configure the Coveo Master server to use and synchronize the index on the Mirror server.

Before proceeding with the following procedure, ensure that the CES mirror components are installed on the Mirror server (see "Installing CES Mirror Components" on page 57).

To configure the Master server to synchronize a Mirror server

1. Using an administrator account, connect to the Coveo Master server.
2. Access the Administration Tool (see "Opening the Administration Tool" on page 256).
3. In the Administration Tool, select **Index > Mirrors**.

4. In the **Mirrors** page, click **Add**.

5. In the **Add Mirror** page:

![Add Mirror page](image)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Name</strong></td>
<td>Enter the exact name that you entered in the <strong>Mirror name</strong> box in the installer <strong>Mirror Configuration</strong> screen when the Mirror components were installed. By default, this is the hostname of the Mirror server.</td>
</tr>
<tr>
<td><strong>Location</strong></td>
<td>Enter the IP address, the host name, or the fully qualified domain name (FQDN) of the server on which the Coveo Mirror components are installed.</td>
</tr>
<tr>
<td><strong>Port</strong></td>
<td>Enter the port number that you specified when you installed the Mirror components. The default value is 52800.</td>
</tr>
<tr>
<td><strong>Index Folder</strong></td>
<td>Enter the path of the folder that will contain the index files on the Mirror server. The default path is built using the hostname.</td>
</tr>
<tr>
<td><strong>Converter</strong></td>
<td>Clear the <strong>Create a converter on a mirror server</strong> check box only when you do not want to create a converter on the Mirror server.</td>
</tr>
</tbody>
</table>

**Example:** You can replicate the folder structure as on the Master server using the form `{same_Drive}:{CES7}\Index\[Mirror_Hostname]`. When the default slice is on the D: drive on the Master server and your Mirror server hostname is CoveoMirror1, enter `D:\CES7\Index\CoveoMirror1`. 

- **Example:** You can replicate the folder structure as on the Master server using the form `{same_Drive}:{CES7}\Index\[Mirror_Hostname]`. When the default slice is on the D: drive on the Master server and your Mirror server hostname is CoveoMirror1, enter `D:\CES7\Index\CoveoMirror1`. 

to use this serve as an additional converter, for example because other converters are already installed on other servers.

**Note:** By default, remote converter components are installed on the Mirror server to share CPU resources during the conversion of documents and, therefore, speed up indexing (see "Installing CES Mirror Components" on page 57).

to use this serve as an additional converter, for example because other converters are already installed on other servers.

**Note:** By default, remote converter components are installed on the Mirror server to share CPU resources during the conversion of documents and, therefore, speed up indexing (see "Installing CES Mirror Components" on page 57).

f. In the Slices section, you can select the location of the slice files on the mirror server:

i. In the Default box, when needed, change the path for the folder containing the index files for the Default slice.

ii. When your Coveo instance has more than one slice (not just the Default), for each additional slice, when needed, edit the path for the folder containing the index files for the slice.

g. When one or more remote indexes are defined in this Coveo instance, in the Remote Indexes section, for each remote index:

i. In the Mirror Hostname box, enter the hostname of the remote index Mirror server that will execute the queries executed on the Mirror server that you are creating.

ii. In the Mirror Port box, when different from the default value (52800), enter the remote index Mirror server port number.

h. Click Save.

6. In the General page that appears for this mirror, in the Status section, click [Synchronize] to start synchronizing the index on the Mirror server.
**Note:** CES 7.0.7183+ (November 2014) You can synchronize a mirror (other than the Default) even when its status is In Sync.

Forcing a synchronization may be useful in rare cases such as when you need to isolate a Mirror server for external reasons or when you realize your Mirror server did not have the same access as the Master server for the security cache updates.

7. Under **Synchronize Mirrors**:

![Image of Coveo Platform 7.0 Administrator Guide](image)

   a. In the **Synchronize from** drop-down list, select **Default on localhost** unless you have another in sync mirror from which you want to synchronize the index.

   b. Select **Use compression** only when the connection between the Master and Mirror servers is slow such as when the servers are connected through a WAN in a GDI configuration. Compression requires more CPU resources.

   c. Click **OK**.

8. In the **General** page that appears again, in the **Status** section, you can monitor mirror synchronization progress, and can abort it if needed by clicking [**Cancel Synchronize**].

![Status Table](image)

When the synchronization is completed, the **Mirror is in sync** status appears.
### What's Next?

Once your Mirror server is up and running and synchronized with the Master server, the next step is to let Front-End servers know that they can send queries to this server (see "Coveo .NET Front-End First Time Setup" on page 47). Also consider one of the following options:

- Add the Mirror server as an alternate server (see "Configuring a .NET Front-End Server to Use Failover Alternate Back-End Servers" on page 100).

  OR

- Include the Mirror server in a network load-balancing (NLB) cluster used by the Front-End servers (see "Configuring Coveo Servers in a Network Load-Balancing Cluster" on page 98).

### 8.6.4.15.2 Adding an Index Slice to the Master Server

Slices are parts of the index data located on separate physical disks. Their main purpose is to increase the available space to index more documents. Slices also contribute to speed up the indexing and querying processes, as they reside on separate disks on the Master server (see "About Index Slices" on page 18).

You need to add one index slice when the number of indexed document in the Default slice on the Master server has reached the limit for one slice. You can have up to two slices, including the original Default slice, on the Master server (see "Coveo Platform Hardware and Software Requirements" on page 3).

**Note:** When the two slices on your Master server are getting full, consider federating search on two or more Coveo instances (see "About Geographically Distributed Indexing" on page 20).

**Note:** The indexing process fills the slices in a distributed fashion. When you add one a slice, because the default slice is getting close to the limit, new documents will be added to the new slices until it reaches the number of documents contained in the default slice. The documents are then distributed evenly to the two slices.

To add an index slice to the Master server

**Tip:** Make sure your index is in Read-Write mode before adding a new slice (see "To manually toggle between the read-write and read-only index modes" on page 263). If you try to add a slice and the UI does not respond, your index is probably in Read-Only mode.

1. On the Coveo Master and, if applicable, Mirror servers, add a hard disk of the necessary size to hold the index slice that you want to add (see "Coveo Platform Hardware and Software Requirements" on page 3).
Important: When your Coveo server topology includes one or more Mirror servers, adding a slice on the Coveo Master server also adds the slice on all Mirror servers. You must therefore ensure that the necessary hard disks are available on the Mirror server(s) before continuing this procedure.

2. On the Coveo Master server, access the Administration Tool (see "Opening the Administration Tool" on page 256).

3. In the Administration Tool, select **Index > Mirrors**.

4. In the **Mirrors** page, click **Add Slice**.

5. In the **Add Slice** page that appears:

   a. In the **Slice Name** box, enter a name to identify the slice.

      **Example:** The original slice is called **Default**. When this is the first slice that you add, you can use **Slice2**. If you need to use all four slices on the Master server, you could then use **Slice3** and **Slice4** to name the other slices.

   b. In the **Slice host for mirrors** section, you configure where the slice is created for the Master server (the **Default** mirror). When your Coveo server topology includes one or more Mirror servers, you must also create the slice on the mirrors (ex.: **CoveoMirror1** in the screen capture).

      i. Select **Create a slice on a mirror server** to create a slice on the Master server, and if applicable, on all Mirror servers.

      ii. In the **Index Folder** box, enter the path of the folder that will contain the index files on the dedicated hard disk that you planned for this slice for the Master server, and if applicable, on all Mirror servers.
**Important:** Each slice must reside on a dedicated hard disk (see "Coveo Platform Hardware and Software Requirements" on page 3). Adding a slice on a hard disk used by another slice defeats the purpose of a slice that is to distribute hard disk I/Os and improve performance for a large index.

**Note:** On a Mirror server, the folder below [Drive]\CES7\Index\ must not be Default. Rather use the Mirror server hostname.

**Example:** For the Default mirror (on the Master server), when the original Default slice is on the D: drive and you installed an E: drive for the new slice, enter E:\CES7\Index\Default\Slice2. When your Coveo server topology includes a Mirror server named CoveoMirror1, you can replicate the folder structure of the Master server, but replace Default by the Mirror server hostname. Enter E:\CES7\Index\CoveoMirror1\Slice2.

**Note:** The index folder can be moved later, but this task is not trivial (see "Moving the Index to a Different Hard Disk Drive" on page 202).

iii. Click **Save**.

CES creates the Slice on the Master server and, if applicable, on the Mirror server(s).

6. In the **Slices** page that appears, verify that a green check mark appears under **Online**, **In Sync**, and **Updates** for the new slice.

---

8.6.4.15.3 Applying an Action to a Mirror

The **More Action** drop-down list in the **Mirrors** page of the Administration Tool regroups actions which can be applied to mirrors.

**Note:** When an action is applied to a mirror, it is also applied to all its related slices.

To apply an action to a mirror

1. On the Coveo Master server, access the Administration Tool (see "Opening the Administration Tool" on page 256).
2. In the Administration Tool, select **Index > Mirrors**.
3. In the **Mirrors** page.
a. Select the check box for the mirror on which you want to apply an action.

b. In the More Actions drop-down list, select the desired action.

For more information concerning available actions on mirrors, refer to the following table.

<table>
<thead>
<tr>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Synchronize</td>
<td>Immediately sends and commits pending transactions from the master to the mirror indexes. It is similar to the Commit Current Transaction button in the Overview page (Status &gt; Overview), but applies to all the selected mirrors; whereas, the Commit Current Transaction button only applies to the main index. Because the content of pending transactions cannot be queried, the Synchronize action must be applied when mirrors are not In Sync.</td>
</tr>
<tr>
<td>Important:</td>
<td>At the end of a mirror server synchronization, the master server switches to read-only mode, and then returns to read-write mode. During the switch that lasts a few minutes, the search interface page is unavailable (queries are disabled). You must thus only synchronize your mirror servers in off-peak search periods.</td>
</tr>
<tr>
<td>Note: CES 7.0.7183+ (November 2014)</td>
<td>You can synchronize a mirror (other than the Default) even when its status is In Sync. Forcing a synchronization may be useful in rare cases such as when you need to isolate a mirror server for external reasons or when you realize your mirror server did not have the same access as the master server for the security cache updates.</td>
</tr>
<tr>
<td>Cancel Synchronize</td>
<td>Cancels the Synchronize action. Important: Synchronization must be re-established as soon as possible, because the content of pending transactions cannot be queried.</td>
</tr>
<tr>
<td>Enable Queries</td>
<td>Allows queries to be sent to the mirror indexes. Queries are accepted as long as the Disable Queries action is not applied.</td>
</tr>
<tr>
<td>Disable Queries</td>
<td>Cancels the Enable Queries action. It is recommended to disable queries when mirrors are not In Sync or updates are disabled, because, in these cases, the index content is not up-to-date.</td>
</tr>
<tr>
<td>Enable Updates</td>
<td>Allows updates to be sent to the mirror indexes. Updates are accepted as long as the Disable Updates action is not applied and the mirror is online.</td>
</tr>
<tr>
<td>Disable Updates</td>
<td>Cancels the Enable Updates action. It is recommended to disable updates when the master index is offline to prevent unnecessary connection attempts.</td>
</tr>
</tbody>
</table>
The statuses of the mirrors are modified accordingly.

8.6.4.15.4 Determining the Status of a Mirror or Slice

The status of mirrors appear in the **Mirrors** page while those of slices appear in the **Slices** page. There are four statuses:

- **Online**
- **In Sync**
- **Queries** (applicable only to mirrors)
- **Updates**

To see the status of the slices

1. On the Coveo Master server, access the Administration Tool (see "Opening the Administration Tool" on page 256).
2. In the Administration Tool, select **Index > Mirrors**.
3. In the **Mirrors** page, click the mirror that contains the slice for which you want to see the status.
4. In the **General** page that appears, in the navigation panel on the left, click **Mirrors** or **Slices**, depending on for which one you want to see the status.
5. In the **Mirrors** or **Slices** page, verify that a green check mark appears under **Online**, **In Sync**, and **Updates** for the new slice.
Note: CES 7.0.7183+ (November 2014) The space between the Port and Online columns can show one of the following mirror warning messages:

- The mirror service is outdated
- Out of disk space
- Synchronizing
- Access denied
- Updating security cache (n%)

6. Refer to the following table for details on each status and possible actions.

<table>
<thead>
<tr>
<th>Status</th>
<th>Description</th>
<th>Online</th>
<th>Offline</th>
<th>Actions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Online</td>
<td>Indicates whether mirrors and slices are online or offline.</td>
<td>Online</td>
<td>Offline</td>
<td>When offline, ensure that:</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>- The Mirror server is up and running.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>- The CES service is running.</td>
</tr>
<tr>
<td>In Sync</td>
<td>Indicates whether mirrors and slices are synchronized or desynchronized.</td>
<td>Synchronized</td>
<td>Desynchronized</td>
<td>To synchronize them (see &quot;Applying an Action to a Mirror&quot; on page 344).</td>
</tr>
<tr>
<td></td>
<td>They are synchronized when pending transactions have been applied to them.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Queries</td>
<td>Indicates whether mirrors accept queries or not. Does not apply to slices.</td>
<td>Accept queries</td>
<td>Do not accept queries</td>
<td>To disable queries (see &quot;Applying an Action to a Mirror&quot; on page 344).</td>
</tr>
<tr>
<td></td>
<td>Note: Because an offline Mirror server cannot accept queries. It is</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>recommended to Disable Queries for a Mirror server that is desynchronized</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>or that does not accept updates because, in such cases, its index content</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>is not up-to-date.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Status</td>
<td>Description</td>
<td>Actions</td>
<td></td>
<td></td>
</tr>
<tr>
<td>--------</td>
<td>-------------</td>
<td>---------</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Updates</td>
<td>Indicates whether the mirrors accept updates or not.</td>
<td>Accept updates</td>
<td>Do not accept updates</td>
<td></td>
</tr>
</tbody>
</table>

**Note:** Because an offline Mirror server cannot accept updates, it is recommended to **Disable Updates** for this mirror to prevent unnecessary connection attempts by the Master server.

8.6.4.15.5 Changing the CES Service Port

You may encounter a situation where you need to change the CES service port for a Coveo server. Select an appropriate port number (see "About the CES Service Port" on page 230).

**Example:** When you plan to upgrade the Coveo Platform from one major version to another, like from version 6.x to 7.x, you can install the two instances on the same Master server, but you need to ensure that the two instances use different CES service port numbers, like 52800 for version 6.x and 52801 for version 7.x.

You need to change the CES service port on the Master server and on each Front-End Server or your Coveo instance.

**To change the CES service port on the Master server**

1. Using an administrator account, connect to the Coveo Master server.
2. Open the Administration Tool (see "Opening the Administration Tool" on page 256).
3. In the Administration Tool, select **Configuration > Advanced**.
4. In the **Advanced** page, change the **Port** value and then click **Apply Changes**.

**To change the CES service port on a Front-End server**

1. Using an administrator account, connect to the Coveo Front-End server.
2. Using a text editor:
   a. Open the [.NET_Front-End_Path]\Web\Web.config file.
   b. In the <coveoEnterpriseSearch> section of the file, change the port value in the following line:

   `<server hostname="localhost" port="52801"
   sslCertificatePath="D:\CES7\Config\Certificates\cert-iis.p12"/>

   c. Save the file.

8.6.4.15.6 When to Add a Mirror?

It is recommended to add a new mirror when the Coveo Master server is slowed down by numerous queries.
Example: If the average query response time for a Coveo server starts to increase when reaching 30,000 queries per hour, create a new mirror when the rate of queries increases by slices of 30,000 queries per hour.

Tip: You can determine the number of queries handled by CES as well as the average querying time from the Administration Tool by selecting Reports > Query History (see "What Information Is Displayed in the Query History?" on page 386).

8.6.4.15.7 What Is Load-Balancing?

Load-balancing is an optimization technique whose purpose is to distribute tasks among servers, disks and CPUs on a network in order to decrease computing time. The balancing process is accomplished by a load balancer—a virtual server which receives tasks and assigns them to physical servers. The clustering and load-balancing service commonly used in Windows environments is Microsoft NLB.

Note: For more information concerning load-balancing with Microsoft NLB, refer to the following Microsoft document: Network Load Balancing Technical Overview.

8.6.4.15.8 Minimizing the Searchability Delay

The searchability delay is the time between when a document is available in a repository and the time it becomes searchable in Coveo search interfaces. Obviously, it is desirable to minimize this delay so that end-users can search for and find documents they created just minutes ago.

Example: Users are used to efficiently search for sent or received emails in the My Emails Coveo search interface, but may get frustrated if they do not find emails sent or received just a few minutes ago.

The index freshness depends on the indexing processing pipeline that involves many operations, each of which can have an impact on the searchability delay. Coveo Enterprise Search offers features like Near Real-Time Indexing that allow you to minimize the searchability delay.

8.6.4.15.8.1 To minimize the searchability delay

1. Ensure sources are refreshed at short intervals.

The refresh rate of a source may have a significant impact on the searchability delay

Ensure that the incremental refresh or refresh schedules are configured with a small time interval, at least for sources for which you want fast searchability (see "Scheduling a Source Incremental Refresh" on page 433 and "Scheduling Source Refresh Actions" on page 435).

Examples:

- The refresh rate of a Microsoft SharePoint legacy Intranet source is set to once a week on Saturdays at midnight. If you modify a document in this Intranet, the change will not be available in search results before the next Sunday morning.

- The incremental refresh rate of a Microsoft Exchange source is set to every 15 minutes. A new email message may therefore enter the index processing pipeline up to 15 minutes after it is created. You could reduce the incremental refresh rate of this source to every 5 minutes to reduce the searchability delay.
2. Ensure the index commits transactions at short time intervals.

   The index commit rate can also add time to the searchability delay. In the CES Administration Tool, ensure that
   the Commit transaction afterminutes parameter is set to a very short time interval such as 1 minute (see
   "Modifying or Using Advanced Index Parameters" on page 366).

3. Enable and configure Near Real-Time Indexing for each back-end server (Master or Mirror) that processes
   queries (see "About Near Real-Time Indexing" on page 350):

   a. Ensure that the Mirror is Online and In Sync (see "Determining the Status of a Mirror or Slice" on page
      346). Synchronize the Mirror when it is not the case (see "Applying an Action to a Mirror" on page 344).

   b. Ensure Near Real-Time Indexing is enabled and optimized (see "Configuring Near Real-Time Indexing"
      on page 351).

8.6.4.15.9 About Near Real-Time Indexing

Near Real-Time Indexing (NRTI) is a feature that improves the index freshness, allowing Coveo Enterprise Search
(CES) to make new documents searchable faster. More precisely, NRTI significantly reduces the index pipeline
processing time, the time between when a new, modified, or deleted document is sent to the index by a crawler and
when the document is searchable by end-users. When a Coveo server meets the requirements, enabling the
NRTI feature easily reduces the index pipeline processing time by one order of magnitude (10 times shorter).

**CES 7.0.7022+ (September 2014)** NRTI is enabled by default for both new and existing indexes, but can be
disabled/enabled from the Administration Tool (see "Configuring Near Real-Time Indexing" on page 351).

The index pipeline processing time may greatly vary depending on numerous factors such as the index size, the
number of new documents to index at a given time, and the available resources on your Coveo Master and Mirror
servers.

**Examples:** For a 40 million document index:

- In a normal scenario where the Coveo server meets the requirements and crawlers send a normal flow of
  new documents to the index, the index pipeline processing time may be reduced from 30 minutes to less than
  3 minutes, respectively without and with the NRTI feature.

- In a worst case scenario where the Coveo server does not meet the requirements and large sources are
  rebuilt on top of a normal flow of new documents, the index pipeline processing time may be of a few days
  and enabling the NRTI feature will most likely not help because the server is lacking resources.

NRTI creates small temporary slices called subslices to receive new, changed, or deleted indexed documents.
Because subslices are much smaller in size than a regular slice of a large index, their index pipeline processing is
completed much faster, allowing to return queried documents they contain much faster.

NRTI applies to all sources of the index, improving the freshness of documents from all sources. NRTI fully supports
marking and collaborative rating, meaning that users can transparently tag or apply collaborative rating to
documents that are available from subslices or normal ones. The subslice management is transparent to a Coveo
administrator, subslices do not appear in the list of slices in the Administration Tool.
Feature History

<table>
<thead>
<tr>
<th>CES version</th>
<th>Monthly release</th>
<th>Features</th>
</tr>
</thead>
<tbody>
<tr>
<td>7.0.7022</td>
<td>September 2014</td>
<td>NRTI enabled by default</td>
</tr>
<tr>
<td>7.0.6942</td>
<td>August 2014</td>
<td>Addition of a NRTI Administration Tool configuration page [more]</td>
</tr>
<tr>
<td>7.0.6830</td>
<td>July 2014</td>
<td>General availability</td>
</tr>
<tr>
<td>7.0.6767</td>
<td>June 2014</td>
<td>Introduction in a beta version</td>
</tr>
</tbody>
</table>

8.6.4.15.9.1 Configuring Near Real-Time Indexing

The Near Real-Time Indexing (NRTI) feature can significantly reduce the index pipeline processing time for indexes of two million documents or more (see “About Near Real-Time Indexing” on page 350). Smaller indexes already offer a short index pipeline processing time, so enabling NRTI when your index is small has no noticeable effect.

When your Coveo deployment includes more than one back-end server, NRTI must be enabled on all Mirrors that are serving queries.

**Example:** Your Coveo deployment consists of a Master server and two load-balanced Mirrors. The Front-End servers are configured to send queries only to the Mirror servers, not to the Master server. In this scenario, you must enable NRTI only on the two Mirrors. There is no point in enabling NRTI on the Default Mirror (Master server) because it does not serve queries.

8.7 To configure Near Real-Time Indexing

1. Ensure that your Coveo Master and Mirror (if applicable) servers meet the requirements for the size of your index.

   Consider following the recommendation to add a NRTI dedicated disk on each server serving queries (see "Coveo Platform Hardware and Software Requirements" on page 3).

2. On the Coveo server, access the Administration Tool.

3. Before enabling NRTI on a Mirror server:
   a. Ensure that the Mirror is **Online and In Sync** (see "Determining the Status of a Mirror or Slice" on page 346).
   b. Synchronize the Mirror when it is not the case (see "Applying an Action to a Mirror" on page 344).

4. On the Administration Tool menu, select **Index > Mirrors**.

5. In the **Mirrors** page, in the **Name** column table, click the mirror for which you want to enable NRTI.

   Repeat the following steps for each mirror for which you want to enable NRTI.

6. In the **Mirror: [name] General** page, in the navigation panel on the left, click **Near Real-Time Indexing**.

7. In the **Mirror: [name] Near Real-Time Indexing** page:
a. If not already the case, select the **Enabled** check box.

For CES 7.0.7022+, NRTI is enabled by default for both new and existing indexes.

b. In the **Index Folder** box, enter the full path where you want to save the NRTI index files.

**Note:** The default folder for new or existing indexes like when the box is empty is \[Index_Path]\Index\Default\RealtimeIndexing so by default, the NRTI files are stored on the same disk as the normal index slices.

Sharing the same disk will work, but because NRTI is an I/O intensive process, to achieve optimal performances, it is recommended to add one dedicated disk for the NRTI files on each Coveo server (Master or Mirror) that are serving queries, and point to this disk with the **Index Folder** parameter. The dedicated disk specifications depend on the size of your index (see "Coveo Platform Hardware and Software Requirements" on page 3).

c. In the **Temporary Files Folder** box, enter the path where the NRTI temporary files are saved.

For an existing index, the default folder that applies when the box is empty is \[Index_Path]\Temp.

d. In the **Maximum Number of Documents per Slice** box, leave the default value (200000) unless Coveo Support instructs you to change it.

This NRTI temporary slice size optimally minimizes the indexing pipeline processing time and the required NRTI resources.

e. **CES 7.0.7022+ (September 2014)** In the **Minimum Number of Documents to Activate** box, enter the index size specified in number of documents, above which the enabled NRTI will start to operate. The default and recommended value is 1000000. The NRTI process starts to improve performances for indexes of about this size. Consult Coveo Support before changing this value.
Note: The documents that are in the index pipeline at the time NRTI is enabled must be indexed before NRTI becomes effective. In a healthy index, this delay will be relatively short, such as 30 minutes for a 40-million document index. In a bad case scenario where the Coveo server is lacking resources and cannot manage to close pending transactions, this delay could be significantly longer.

8. Estimate the index pipeline processing time.

The following steps give a method to estimate how long it takes to complete the index pipeline process.

a. On the Coveo server, using Windows Explorer, open the folder of the regular slice. If there is more than one slice, open the folder of each slice.

Example: By default, the first slice is called Default and its folder is: [CES_Path]\Index\Default\Default

b. In the slice folder(s), look for pre-transaction and transaction files that are named respectively using the following patterns:

    • Index-nnnnnnnnn.ptn
    • Index-nnnnnnnnn.trn

where nnnnnnnnn is an incremental transaction ID number.

Note: When no documents are being indexed, no pre-transaction and transaction files will be present in the slice folder(s). Either force a source refresh/rebuild or wait for some source to get refreshed to see new transaction files appear.

c. At a given time, note the highest transaction ID number (without the leading zeroes) from the slice folder(s), and also note the current time.

d. Using an account and a Coveo search interface having access to all the indexed content, in the search box, repeatedly submit the following query until you start getting results:

    @systransactionid >= [highest_transaction_id]

Example: At 14:05, the pre-transaction or transaction file in the slice folders with the highest transaction number is Index-0000005044.trn.

In the search interface, you type the following query:

    @systransactionid >= 5044

Note: When no documents are being indexed, no pre-transaction and transaction files will be present in the slice folder(s). Either force a source refresh/rebuild or wait for some source to get refreshed to see new transaction files appear.

e. Note the time at which you start getting results, and then subtract the time at which you noted the highest transaction ID to get an estimate of the index pipeline process time.

What's Next?

Ensure that all CES aspects are optimized to minimize the searchability delay (see "Minimizing the Searchability Delay" on page 349).
8.7.0.0.1 Configuring the Search Web Service for a Mirror

Coveo Enterprise Search comes with a Search Web Service (see "About the Coveo Search Web Service" on page 231). The Search Web Service needs to be enabled and configured only when a custom search application uses it to perform search operations.

The Search Web Service is enabled by default on a Coveo Master server and disabled by default on Mirror servers. You can enable/disable and configure the Search Web Service independently for each server. The Search Web Service is secured using certificates.

To configure the Search Web Service for a Coveo Mirror Server

1. On the Coveo server, access the Administration Tool.
2. In the Administration Tool, select Index > Mirrors.
3. In the Mirrors page, click the name of the mirror for which you want to configure the Search Web Service.
   
   Note: The index of the Coveo Master server is represented here as a mirror typically named Default.

4. In the page for the selected mirror:
   
   a. In the navigation panel on the left, select Search Web Service.
   b. Select/clear the Enabled check box to enable/disable the Search Web Service for the selected mirror.
Tip: When no custom application uses the API, it is a good practice to disable the API, particularly when the Use SSL Connection option is cleared, to prevent anonymous Search Web Service accesses.

Note: The Search Web Service is enabled by default on a Coveo Master server and disabled by default on Mirror servers.

c. Select the Keep Alive check box to use a single TCP connection to send and receive multiple HTTP requests/responses, as opposed to opening a new connection for every single request/response pair.

Selecting this option can improve performances, more notably when Use SSL Connection is selected by preventing repeating the SSL handshake for each request/response pair.

d. In the Port box, you can change the port number used to access the Search Web Service on this mirror. The default is 52810.

You must change the port when the default port is used by another application and may need to change it for example to respect your IT standards. When you have more than one mirror, each mirror may use the same or different ports.

e. In the Number of Threads box, you can change the minimum number or threads that are allocated to concurrently serve requests to the Search Web Service. The default is 10.

f. In the Error Log box, enter the path and file name in which Search Web Service logs will be written. No logs are saved when the box is empty.

g. Select the Use SSL Connection check box to only accept Secure Sockets Layer (SSL) connections to the Search Web Service. Clear to use non-secured connection (HTTP).

h. When the Use SSL Connection option is selected, leave the Certificate, Certificate Private Key, and Trusted CAs boxes empty to use the default CES certificate files. Otherwise, enter the paths and file names where your own appropriate certificate files are on the Coveo server.

i. Click Apply Changes.

Note: When you change the configuration for a Mirror server, the changes are effective within about a minute when the next transaction is committed.

5. When you enable/disable Search Web Service on a remote mirror, your need to restart the CES service on the mirror server for the modifications to be effective.

8.7.0.1 Administration Tool - Remote Indexes Menu

This section regroups topics showing you how to manage connections for a Coveo instance to remote CES indexes from which additional query results can be collected.

8.7.0.1.1 Adding or Modifying Remote Indexes

When two or more Coveo instances co-exist within an organization, you can use the remote index feature to set up geographically distributed indexing (GDI) (see “About Geographically Distributed Indexing” on page 20).
You can configure a .NET search interface attached to one Coveo instance to send queries to a remote Coveo instance. The local Coveo instance merges and ranks results received from both the local and remote indexes (see "Setting up Geographically Distributed Indexing" on page 21).

The following procedure describes how to add or modify remote indexes in the Administration Tool for a Coveo instance from which you want to query remote indexes.

**Note:** You can add several remote indexes by repeating the following procedure. The remote indexes defined will not be automatically queried. You must also add a remote index to the scope of a .NET search interface from which you want to receive remote index results (see "Configuring the Scope of a .NET Search Interface" on page 597).

To add or modify a remote index

1. Connect to the Coveo Master server of the Coveo instance from which you want to query a remote index.
2. Access the Administration Tool (see "Opening the Administration Tool" on page 256).
3. In the Administration Tool, select Index > Remote Indexes.
4. In the Remote Indexes page, perform one of the following actions:
   a. To add a new remote index, click Add.
   OR
   
   b. To modify an existing remote index, click the name of the appropriate server.
5. In the Add Remote Index or existing remote index page:

   a. In the Name box, enter a name that identifies this remote index. The name must not include spaces.

   This name will appear in the .NET Interface Editor in the page where you can configure the scope of a .NET search interface and will not be visible by end-users in .NET search interfaces.
b. In the **Description** box, enter a description for the remote index (ex.: content, location, etc.) to help you uniquely identify this remote index.

c. **Under Services Information:**
   
i. In the **Services Host** box, enter the host name for the Master server of the Coveo remote index.
   
ii. In the **Services Port** box, if different from the default value (52810), change the port for the Coveo Web service port on the remote index server.

   **Note:** Do not confuse this port with the CES service port (52800 by default).

iii. In the **Instance Name** box, in the rare case where your remote index instance name is different from default, enter the correct instance name.

   **Tip:** At the end of the .NET search interface URL for the remote Coveo instance, add the ?&Debug=1 argument to get debug information containing the Instance, Mirror, and Physical index name (see "Getting Debug Information from a .NET Search Interface" on page 135).

iv. Click **Validate**.

   **Note:** If a connection error message appears at the top of the page, verify that on the Coveo remote Master server, the firewall allows incoming connections to the **Services Port**.

   **Example:** Error message example:

   ```
   Could not connect to http://YourServerName:52810/7.0/CoveoAdminService. TCP error code 10060: A connection attempt failed because the connected party did not properly respond after a period of time, or established connection failed because connected host has failed to respond.
   ```

When the remote server responds, a few more parameters appear in the **Services Information** section to specify the credentials of an administrator account to use on the remote Coveo Master server to be allowed to configure the remote index.
v. In the Services Security Provider drop-down box, select the Coveo security provider that can resolve the administrator credentials on the remote Coveo server.

Select Active Directory when your administrator account is a Windows account.

vi. In the Services User Name box, enter the user name of the administrator account.

vii. In the Services User Password box, enter the administrator account password.

viii. Click Validate Credentials to verify that the credentials allow a connection to the web services on the remote Coveo server.

d. In the Local to Remote Mirror Mapping section, for each local mirror, you can specify to which remote mirror the queries will be sent:

```
[Diagram showing Local to Remote Mirror Mapping]
```

1. Local mirror
2. Selection of remote mirror to which queries are sent

**Note:** By default the index on a Master server is referred to as the Default mirror.

- Choose the Select a mirror option and then in the drop-down list, select one of the available remote instance mirrors.

  OR

i. Choose the Configure mirror manually option.

ii. In the Mirror Hostname box, enter the hostname of the Mirror server to which you want to forward queries.

iii. In the Mirror Port box, when different from the default (52800), enter the CES service port for the Mirror server to which you want to forward queries.
**Example:** A local Coveo instance has one Front-End server that sends queries to the Master server, while a second Front-End sends its queries to a Mirror server. You want to add a remote index that has two Mirror servers. Because the remote Master server is often busy indexing content, you want to forward the queries sent to the local Master server (Default mirror) to the remote Mirror1 mirror and the queries sent to the local Mirror1 mirror to remote Mirror2 mirror.

What's Next?

On the Coveo Front-End server of the local Coveo instance, add the remote index to the scope of a .NET search interface (see "Configuring the Scope of a .NET Search Interface" on page 597).

8.7.0.1.2 Troubleshooting 401 Error with Remote Indexes

A 401 error message can appear in the .NET search interface when attempting to connect to a remote index. This may be due to the fact that NTLM is not the default authentication in IIS.

To resolve the 401 error problem in IIS 7

1. Using an administrator account, connect to the Coveo Front-End server.
2. Open the Internet Information Service (IIS) Manager.
3. In the Connections panel, under Sites, select Coveo Enterprise Search 7.
4. In the main panel, double-click Authentication.
5. In the Authentication panel, select Windows Authentication.
6. In the Actions panel, select Provides.
7. In the Providers dialog box, when NTLM is not present in the Enabled Providers list:
   a. In the Available Providers drop-down list, select NTLM, and then click Add.
   b. Click OK.
To resolve the 401 error problem in IIS 6

1. Using an administrator account, connect to the Coveo Front-End server.
2. Open a command line window.
3. Run the following command: `cscript adsutil.vbs set w3svc/NTAuthenticationProviders "NTLM"`

**Note:** Refer to the following Microsoft document for details: How to configure IIS to support both the Kerberos protocol and the NTLM protocol for network authentication.

### 8.7.0.1.3 Logging on as a Batch Job

In some cases like when setting up a remote index, ensure that the CES search application account has the log on as a batch job privilege as follows.

**To log on as a batch job account**

1. Start the **Local Security Settings** application (Windows **Start > Administrative Tools > Local Security Policy**).
2. In the **Local Security Settings** application:
   a. Expand **Security Settings** and **Local Policies**.
   b. Double-click **User Rights Assignment**
   c. In the main list, double-click **Log on as a batch job**.
   d. In the **Log on as a batch job Properties** dialog box, when the CES search application account is not present in the list:
      i. Click **Add User or Group**.
      ii. Select the appropriate user in the dialog box that appears, and then click **OK**.
      iii. Click **OK**.

### 8.7.0.2 Administration Tool - Search Scopes Menu

**CES 7.0.5639+ (July 2013)**

You can centrally define one or more search scopes on the Coveo Master server so that you can easily assign them to .NET search interfaces from one or more Coveo Front-End servers without having to duplicate the search scope definitions (see "Configuring the Scope of a .NET Search Interface" on page 597).

#### 8.7.0.2.1 What Are Search Scopes?

**CES 7.0.5639+ (July 2013)**

Each Coveo .NET search interface has a specific scope that you can configure from the .NET Interface Editor (see "Configuring the Scope of a .NET Search Interface" on page 597). This normal .NET search interface scope is transparent to the end-user.
On the Coveo Master server, you can also centrally define one or more search scopes so that you can later assign to .NET search interfaces from one or more Coveo Front-End servers. Search scopes are defined using filter expressions and/or collections on the local and/or remote Coveo indexes.

When two or more search scopes are assigned to a .NET search interface, the Search In facet automatically appears in the .NET search interface to allow end-users to easily switch between search scopes without having to select another .NET search interface.

Example: In your Los Angeles head office, you can create search scopes that exclusively search in the Boston and Paris remote indexes within your organization. End-users can select the desired search scope when needed from the Search In facet that appears in the .NET search interface.

Search scopes are useful when included in a .NET search interface that has a large scope (such as the out-of-the-box All Content.NET search interface) or when you want to include one or more remote indexes. When you plan to assign more than one search scope to a .NET search interface, you typically define search scopes with mutually exclusive scopes so that an end-user can toggle the search between these separate contents.

Note: CES 7.0.5556– (June 2013) Use the deprecated custom search feature (see "Configuring a Custom Scope With the .NET Interface Editor" on page 633).

What's Next?

Centrally defines one or more search scopes using the Administration Tool (see "Adding a Search Scope" on page 361).

8.7.0.2.2 Adding a Search Scope

CES 7.0.5639+ (July 2013)

You must create search scopes on the Coveo Master when you want to assign them to a .NET search interface from a Coveo Front-End server (see "What Are Search Scopes?" on page 360).

Note: CES 7.0.5556– (June 2013) Use the deprecated custom search feature (see "Configuring a Custom Scope With the .NET Interface Editor" on page 633).

To add a search scope

1. On the Coveo server, access the Administration Tool.
2. In the Administration Tool, select Index > Search Scopes.
3. In the Search Scopes page, click Add.
4. In the Add Search Scope page:
a. In the **Name** box, enter a name for the search scope.

   **Note:** This name will appear in the .NET Interface Editor when assigning a search scope to a .NET search interface (see "Configuring the Scope of a .NET Search Interface" on page 597).

b. In the **Description** box, optionally enter information to help you understand the purpose of this search scope.

c. Select the **Exclude Local Mirror** check box when you want this scope to only refer to remote indexes defined in the **Additional Indexes to Search** section of this page.

d. In the **Local Filter Expression** box, enter the filter expression that define this search scope.

   This expression is only applied to the local index so it is disabled and has no effect when the **Exclude Local Mirror** check box is selected.

   **Example:** You want to create a search scope to narrow search to your SharePoint Intranet source. Enter the following filter expression that uses field query:

   `@syssource=Intranet`

e. Next to **Collections**, when you want to narrow the search scope to one or more collections of your local index, select the check box for the appropriate collection(s).

   You cannot select collections when the **Exclude Local Mirror** check box is selected.

f. In the **Additional Indexes to Search** section, when you want to include content from one or more remote...
indexes (other Coveo instances within your organization) in this search scope:

<table>
<thead>
<tr>
<th>Additional Indexes to Search</th>
</tr>
</thead>
<tbody>
<tr>
<td>Index</td>
</tr>
<tr>
<td>🌈 Add Remote Index</td>
</tr>
</tbody>
</table>

i. Click **Add Remote Index**.

ii. In the **Index** column, select the remote index to include.

Note: When the drop-down list in the **Index** column is empty, you must first define one or more remote indexes accessible to this local Coveo instance (see "Adding or Modifying Remote Indexes" on page 355).

iii. In the **Filter Expression** column, optionally enter a filter expression to narrow search results from this remote index.

iv. In the **Collections** column, optionally select the check box for one or more collections from this remote index for which you want to narrow the search scope.

v. In the **Execution Time (sec)** column, enter a timeout value in seconds to wait for results from this remote index before aborting the search. When you enter 0, the search interface waits indefinitely.

Example: When a WAN connection separates the local and remote indexes, you can enter 3 (sec) to prevent the .NET search interface using this search scope from freezing when the connection is overloaded and delaying the return of the remote search results.

g. Click **Save**.

What's Next?

- Consider setting one of your search scopes as the default scope (see "Setting a Default Search Scope" on page 363).

- Assign the search scope to the appropriate .NET search interface(s) on one or more Coveo Front-End servers (see "Configuring the Scope of a .NET Search Interface" on page 597)

8.7.0.2.3 Setting a Default Search Scope

Once you defined one or more search scopes (see "Adding a Search Scope" on page 361), you can set one of them as the default search scope.

In the .NET Interface Editor, when a default search scope is defined from the Administration Tool, you can select the **Use the Default Scope from the Administration Tool** option to assign the default search scope to a .NET search interface (see "Configuring the Scope of a .NET Search Interface" on page 597). In this case, if you change the default search scope from the Administration Tool, all .NET search interfaces to which the default search scope is assigned will be automatically updated.
To set the default search scope

1. On the Coveo server, access the Administration Tool.

2. In the Administration Tool, select **Index > Search Scopes**.

3. In the **Search Scopes** page:
   
   a. Select the check box in front of the search scope that you want to set as the default search scope.
   
   b. Click **Set as Default**.

   A **Default** button appears next to the search scope to identify that it is the default search scope and to allow you to revoke its default status.

8.7.0.3 Administration Tool - Result Clustering Menu

Result clustering modifies the way search results are displayed. When result clustering is enabled, groups are created. When clicking a group, a query is performed and the documents concerning the group in question are displayed.

**Example:** For the query **CES AND Help**, result clustering is likely to regroup search interface help documents in one cluster, Administration Tool help documents in another, etc. Whereas, ranking without result clustering displays those documents by relevance score only (ex.: two search interface documents can be separated by an Administration Tool and an Interface Editor one).

By default, result clustering is disabled. You can enable and configure results clustering (see “Enabling and Customizing Result Clustering” on page 364).

8.7.0.3.1 Enabling and Customizing Result Clustering

Result clustering regroups the most relevant search results by similarities in order to allow quick identification of pertinent documents on the same subject. Clusters are created using an algorithm which identifies similarities between document concepts, excerpts or summaries (depending on the **Clustering Source** selected).

You can specify the minimum and maximum number of clusters to create as well as the maximum number of results to analyze for clustering. However, the exact number of clusters produced is determined by the variety of keywords and document types identified by the result clustering algorithm.
By default, result clustering is disabled in the index. When you enable it, the Cluster regroups the most relevant search results by similarities to allow quick identification of pertinent documents on the same subject.

**Note:** Result clustering is used transparently in the .NET search interface (i.e. groups of results are not identified).

To enable and customize result clustering

1. On the Coveo server, access the Administration Tool.
2. In the Administration Tool, select **Index > Result Clustering**.
3. In the **Result Clustering** page:

   a. In the **Enabled** section, select the **Result clustering enabled** check box.

   b. In the **Minimum Number of Clusters** box, modify the minimum number of clusters to create. The value must be between 1 and 1000. This value is used when documents returned by a query are similar.

   c. In the **Maximum Number of Clusters** box, modify the maximum number of clusters to create. The value must be between 1 and 1000. This value is used when documents returned by a query are numerous and heterogeneous.

   d. In the **Maximum Number of Results for Clustering** box, enter the maximum number of results to analyze for clustering. The value must be between 1 and 1000. Documents not analyzed are sorted by relevance score. If a query returns fewer results than the number entered, all documents are subject to clustering.

   **Note:** If the value in the **Minimum Number of Clusters** box is high, the value in the **Maximum Number of Results for Clustering** box must equally be high; otherwise, clusters containing only one result can be created (to users, it looks like clustering is not used).

   **Note:** Clustering requires considerable CPU resources; therefore analyzing more results than the default value of 100 can slow down Coveo Enterprise Search (CES).

   e. In the **Clustering Source** drop-down list, select the source to use for clustering.
The result clustering algorithm compares concepts, excerpts or summaries of documents:

- Concepts are words recognized as important by linguistic algorithms.
- Excerpts are groups of passages containing the terms queried.
- Summaries are complete sentences recognized as important by an advanced linguistic algorithm. They are more precise than concepts, but require more CPU resources to be extracted. Summarization can be disabled for certain sources in order to speed up indexing.

f. Click **Apply Changes**.

What's Next?

Once enabled in the index, in a .NET search interface, you can refine search results using the Refine by Cluster facet.

8.7.0.4 Administration Tool - Advanced Menu

As a Coveo Platform administrator, you can use the **Advanced** page to adapt CES to different network environments and force the processing of some background processes such as the rebuild of the Word Corrector Lexicon.

8.7.0.4.1 Modifying or Using Advanced Index Parameters

You can modify or use advanced index parameters to adapt CES to different network environments and force the processing of some background processes that are performed asynchronously by default.

To modify or use advanced index parameters

1. On the Coveo server, access the Administration Tool.

2. Select **Index > Advanced**.

3. In the **Advanced** page, modify or use the advanced index parameters presented in the following screen capture and table, and then click **Apply Changes**.
Optimization

Determines the number of results subject to a second, more precise ranking—this second ranking insures that only the most pertinent documents are displayed on top of the result list. Values between 2 and 1,000 are accepted. The default is 100.

Note: This process requires considerable CPU resources. Increasing the value of this field above 100 documents can slow down the querying process. To speed up CES, it is possible to limit the extra ranking process to 20-50 documents. This is usually sufficient as the average user rarely displays more than two result pages.
<table>
<thead>
<tr>
<th>Section</th>
<th>Description</th>
</tr>
</thead>
</table>
| Transactions  | The Commit transaction after \( n \) [Seconds](CES 7.0.6942+ (August 2014)), [Minutes](CES 7.0.6942+ (August 2014)), [Hours](CES 7.0.6942+ (August 2014)) parameters specify at what time interval a transaction is committed even if it has not reached its maximum size limit (see “What Is a Transaction?” on page 259). The default value is 1 minute. It is appropriate for normal index operations where existing sources are continuously refreshed, allowing new documents to be processed quickly, and therefore not limiting the index freshness. When the searchability delay is an issue and near-real-time indexing is enabled, you can consider setting a sub-minute value in seconds (see “About Near Real-Time Indexing” on page 350). The main inconvenience of having short intervals is that crawlers are stopped shortly at each transaction commit. You should increase the value only while you initially build or rebuild very large sources.  

**Example:** While you rebuild a 50 million document Exchange source, it is recommended to set a higher commit transaction time limit (ex.: 30 minutes) so that each transaction efficiently writes large amounts of data to the index.  

**Note:** If a transaction is not written in the index, its content cannot be queried.  

| Performance Mode | Determines if a majority (2/3) of the memory cache size is to be allocated for querying or indexing. It is also possible to allow equal resources (1/2 of the memory cache size) to each process. In which case, it is recommended to increase the memory cache available, so each process has access to sufficient memory.  

**Example:** When 50 MB of memory cache is available, and **Optimize for indexing** is selected, then 33 MB are available for indexing (2/3 of the memory cache) and 17 MB for querying (1/3 of the memory cache). When **Optimize for indexing and querying** is selected, 25 MB is devoted to each process (1/2 of the memory cache).  

The value in the **Memory cache size** box determines the maximum memory size limit to force the commit of transactions.  

**Note:** Increasing the memory cache available for indexing and querying slows down other system processes (ex.: index).  

| Field Alias Set | Provides equivalent names for fields (when CES is unable to find a field name in the CES7 database, it searches for alias sets). The **Default Aliases** set comprises alternate names for the built-in fields.  

**Example:** **author** is an alias for **sysauthor**, because users tend to forget **sys** before field names (i.e. a query for @author returns the same results as a query for @sysauthor).  

You can add new field aliases or create different field alias sets in the **Field Alias Sets page (Configuration > Field Aliases)** (see “Managing Field Aliases” on page 506).  

**Notes:**  
- Only one field alias set can be used on the index at a time.  
- **CES 7.0.6547–(March 2014)** You must restart the CES service to make a field alias set change effective.
<table>
<thead>
<tr>
<th>Section</th>
<th>Description</th>
</tr>
</thead>
</table>
| Multiple Value Fields        | A multiple value field is a field that can contain two or more values that are considered independent. When a multiple value field is used to create a facet in the search interface, its values are listed separately in the facet. The Value Separators box allows you to change or add characters recognized as separators of independent field values. You can add more than one value separators. Example: ; , :  
  
  The default character (;) should be used for all built-in fields. Other repositories such as databases or in-house applications could use different separators. Important:  
  - When you change or add Value Separators, a rebuild of all your sources is necessary for the modifications to take effect.  
  - Changing or adding Value Separators characters can break existing field value separations. Contact Coveo Support for assistance before attempting to change this parameter. |
| Enable Wildcards             | Allows the usage of Wildcard characters in queries. In Number of Leading Chars, enter the minimum number of leading characters that the user must enter before a wildcard character. The default is 2. It is not recommended to use a value below two as this would result in computationally expensive wildcard queries. In Number of candidates, specify the number of potential replacement terms for a wildcard expression. Increasing the value can affect performance. The default value is 32. You can safely increase this value to 128. Note: Wildcard queries on the entire content of an index will always take longer to return results. For content where wildcards are appropriate, you should consider isolating the data in a field, and using the field for the wildcard search. |
| Facet cache                  | Specifies the amount of memory to allocate to facet caching.                                                                                                                                                                                                                                                                             |
| Stemming                     | The calculation of the stem classes for queried words is automatically performed during off-peak hours to reduce the indexing time. You can however initiate this calculation for all indexed terms at any time by clicking Perform advanced analysis on language stemming classes. Example: After re-indexing large sources, you may want to not wait until the next off-peak period to update the stem classes. Important: Forcing the calculation of all indexed terms by clicking Perform advanced analysis on language stemming classes may require significant computing resources. |
| Word Corrector Lexicon       | The index maintains a word correction lexicon (WCL) that sorts indexed terms by their number of occurrences and is used by the spelling suggestion algorithm of the query correction feature to find more frequent spelling variants and propose a correction (see "Query Correction Feature" on page 273). The word correction lexicon calculation is performed during off-peak hours to reduce the indexing time. You can however initiate this processing at any time by clicking Rebuild Word Corrector Lexicon. |

8.7.1 Administration Tool - Content Tab

The Content tab contains three menus from which you can see the index structure and find and review detailed information such as security about indexed documents. The features of the Content tab are useful to troubleshoot indexing and search results issues.
Content

The Index Content page displays the tree structure of the master and mirror indexes. Collections can be expanded by clicking ▼. Clicking an index (ex.: Default) displays its properties, clicking a collection displays its Sources and Collections page, and clicking a source displays its Status page (see "Administration Tool - Index Content Menu" on page 370).

Browser

The Index Browser page offers a search interface to easily find and select one or more indexed documents on which you can perform various actions (see "Administration Tool - Index Browser Menu" on page 372).

Security Browser

The Security Browser page offers controls to review the relationships between security entities (see "Using the Security Browser" on page 383).

8.7.1.1 Administration Tool - Index Content Menu

The Index Content page is useful to easily review the structure of collections/sources in the local/remote indexes and the real-time state of remaining documents to be processed for each indexed element.

The Index Content page presents the indexes as expandable tree structures of the form:

- Local Index
  - Master index (typically Default)
    - Collection
    - Source
  - Mirror index 1
    - Collection
    - Source
- [Remote Index 1]
  ...
- [Remote Index n]

The Index Content page presents the real-time status of each tree element as well as the number of documents that need to be processed.
Example: In the following capture, the local index has no mirrors and the SanFranciscoCoveoIndex remote index is listed but cannot be expanded because it is currently unavailable.

In the Index Content page, you can:

- Expand master/mirror indexes as well as collections by clicking the icon.
- Click a master/mirror index to display its property page (Index > Mirrors > General).
- Click a collection to display its information page (Index > Sources and Collections).
- Click a source to display its status page (Index > Sources and Collections > Status).

On the toolbar:

- Click Delete Index Content to delete all the indexed documents, but keep the index configuration (collections, sources, document types...).
- Click Export to create a Microsoft Excel spreadsheet containing the information available from the Index Content.

Note: A remote index running on a CES version different from that of the local Coveo instance appears in the Index Content page but you cannot expand it to review its details.
8.7.1.2 Administration Tool - Index Browser Menu

The Index Browser page is a search interface that allows you to easily find and select indexed documents for which you want to find information or on which you want to apply actions. The Index Browser page is a useful and flexible index maintenance tool as it allows you to apply actions on a single document, on multiple selected documents, or on documents contained in one or more selected folders.

**Tip:** You can access the Index Browser from the source Status page by clicking [Details] under Number of Documents (see “What Information Is Displayed in the Status Page?” on page 289).

**CES 7.0.6547+ (March 2014)** Once in the Index Browser, you can conveniently navigate back to the source Status page by clicking the back to source icon and link.

**Note:** Because browsing the index can expose sensitive information, the Index Browser page is accessible only to a Coveo administrator that is a member of the System Administrator or Index Browser role (see "About Administration Roles" on page 406).

8.7.1.2.1 Index Browser Available Actions

Using the Index Browser, you can perform a number of actions on one or more documents or folders.

The following conditions affect the availability of some of the actions:

- **Contents:**
  - [www.coveo.com](http://www.coveo.com)
Source type must support the action.

User must have required permissions (see "About Administration Roles" on page 406).

Some actions are unavailable when indexing is disabled (see "Disabling or Enabling Indexing" on page 269).

The following table presents the actions that you can apply as a function of the document selection type from the Index Browser.

<table>
<thead>
<tr>
<th>Actions</th>
<th>Description</th>
<th>Single document</th>
<th>Multiple documents</th>
<th>One or more folders</th>
</tr>
</thead>
<tbody>
<tr>
<td>Refresh</td>
<td>The selected document(s) or folder(s) that were modified since the last indexing are deleted and re-indexed.</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Rebuild</td>
<td>The selected document(s) or folder(s) are deleted from the index, and then re-indexed.</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Remove from Index and Add Exclusion Filters</td>
<td>The selected document(s) or folder(s) are removed from the index and an exclusion filter is created to prevent their re-indexing (see &quot;Adding or Modifying Source Filters&quot; on page 295).</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Add an Exclusion Filter</td>
<td>The selected document(s) or folder(s) are subjected to an exclusion filter. However, they are not deleted until the next refresh or rebuild.</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Remove from index</td>
<td>The selected document(s) or folder(s) are removed from the index. They are re-indexed if a rebuild or refresh is performed, because no exclusion filter is created for their path.</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Add Top Result</td>
<td>A Top Result is created for the selected document(s) and a dialog box appears to let you enter the corresponding queries.</td>
<td>✓</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>View Source</td>
<td>The Administration Tool Status page appears for the source containing the document to allow you to review the source state (see &quot;What Information Is Displayed in the Status Page?&quot; on page 289).</td>
<td></td>
<td></td>
<td>✓</td>
</tr>
</tbody>
</table>

What's Next?

Apply an action on one or more documents or folders:

- "Applying an Action on a Document From the Index Browser" on page 380
- "Applying an Action on Multiple Documents From the Index Browser" on page 380
8.7.1.2.2 Finding Documents Using the Index Browser

The Index Browser offers a search interface that allows you to browse the index content and to easily find any indexed document.

To find documents using the search interface of the Index Browser

1. On the Coveo server, access the Administration Tool.

2. In the Administration Tool, select Content > Index Browser.

3. In the Index Browser page:

   a. In the search box, optionally type one or more keywords that the documents you are looking for may contain, click the search button, and then review the search results.

   b. When needed, use the available facets to narrow the search.
8.7.1.2.3 Reviewing Document Details from the Index Browser

You can use the Index Browser to review detailed information for any indexed document.

To review document details from the Index Browser

1. In the index Browser, locate the document for which you want to review details (see “Finding Documents Using the Index Browser” on page 374).

2. In the search results, click Details below the document.

3. In the information panel that appears, select the Properties tab to review the properties associated with the document.

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Printable URI</td>
<td>Link presented in the search results to display</td>
</tr>
<tr>
<td>Clickable URI</td>
<td>Link that is opened when the document is clicked</td>
</tr>
<tr>
<td>Cached version</td>
<td>Link to open the Quick View version of the</td>
</tr>
</tbody>
</table>
<pre><code>                                                             | document in a new window. |
</code></pre>
<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Title</td>
<td>Title given to a document by its author in the document properties. For more information about giving a title to a document, refer to the documentation of the application used to create the document (ex.: Microsoft Word, Adobe Acrobat Pro). The document title and the document filename can be different and are stored in separate fields.</td>
</tr>
<tr>
<td>Author</td>
<td>Author of a document. The author of a document is the user logged onto the workstation when the document is created. The author name can be modified in the document properties. For more information about modifying the author of a document, refer to the documentation specific to the application.</td>
</tr>
<tr>
<td>Content Type</td>
<td>File type of the document.</td>
</tr>
<tr>
<td>Language</td>
<td>Language extracted by the Coveo Platform for a document.</td>
</tr>
<tr>
<td>Size</td>
<td>Size, in bytes, of the document original file.</td>
</tr>
<tr>
<td>Modified Date</td>
<td>Creation or last modification date of the document.</td>
</tr>
<tr>
<td>Indexed Date</td>
<td>Date the document was added to the index.</td>
</tr>
<tr>
<td>Duration</td>
<td>Duration for audio or video documents.</td>
</tr>
<tr>
<td>Attachment</td>
<td>Whether the document is an attachment or not.</td>
</tr>
<tr>
<td>Contains attachments</td>
<td>Whether the document contains attachments or not.</td>
</tr>
<tr>
<td>Reference</td>
<td>Whether the document was indexed by reference (only file information) or content (see &quot;What Is the Difference between Indexing by Reference and Indexing by Content?&quot; on page 481).</td>
</tr>
<tr>
<td>Copy protected</td>
<td>Whether the document is protected against unauthorized duplication or not. Copy protection is common on commercial PDF, audio, or video documents.</td>
</tr>
</tbody>
</table>

**Note:** The content of copy protected documents is searchable, but will not be displayed in a search result to prevent showing it in a context where users can make a copy.

**Example:** With Adobe Acrobat Pro, in the Password Security Settings dialog box, when you clear the **Enable copying of text, images, and other content** check box, the document becomes copy protected, and users viewing it in Acrobat will not be able to copy its content.

In a search result, the file name appears at the place of the title, and the excerpt and Quick View are not available.
Note: When the account you use to access the Administration Tool does not have the permissions to see an indexed document, the following message appears in its Properties tab:

You do not have the permissions to view the document properties.

An account member of the System Administrator (Full Access) role has access to properties for all indexed document (see "About Administration Roles" on page 406). Consider making your account a member of this role (see "Assigning Users to Administration Roles" on page 412).

4. In the information panel, select the Permissions, to review the users/groups associated with the document, their source security provider, and if they are allowed to see the document in search results.

Tip: The content of the Permissions tab is very useful to help understand or troubleshoot why a document is visible or not in search results for a given user or group of users.

Click the Display drop-down list to select either the Effective Combined Permissions or one specific permission set under a permission level to list the corresponding security entities and understand why a user sees a document or not (see "Permission Levels and Sets" on page 223).

Click a security entity to open it in the Security Browser page and review the security entity members (see "Using the Security Browser" on page 383).

Review this column to identify the type of each security entity.

Review this column to identify the type of security provider with which each security entity was retrieved.
Review this column to see if a security entity allows seeing the document or not in search results.

Type in the Filter box to easily refine the list of security entities to the ones containing the typed string. This feature is useful to quickly find a specific security entity or field in long lists.

Notes:

- Since each CES server (master and mirrors) has a security cache instance, security identities can differ from a CES server to another.

  When not a member of any group, a user is known by the security cache instance of servers on which it has performed at least one query. Considering document effective permissions are computed on the master server, a specific user can be missing on a document effective permissions if the user never performed a query on the master server.

  Yet, the missing user can see the document in search results on a mirror server. In such case, to see the user in the document effective permissions, the user only has to perform a query on the master server.

- An internal Anonymous permission was introduced to allow security providers to match a repository anonymous user (such as extranet\anonymous) and consequently, allow any user to see anonymous repository content in search results.

- CES 7.0.7104– (October 2014) The Anonymous permission can misleadingly appear with the denied icon (--) in the Allowed column when it was not set.

- CES 7.0.7183+ (November 2014) The Anonymous permission appears only when it is explicitly allowed.

5. In the information panel that appears, select the Fields tab to review the Name, Type, and Value of fields indexed for the document. The available fields vary depending on the type of source and the built-in or custom field set used (see "Adding or Modifying Custom Fields" on page 494).
Notes:

- Fields are displayed in the document properties only if:
  - They contain a value (ex.: @syslanguage is displayed only if the language of the document is recognized by CES).
  - They are set as a display field.
- CES 7.0.6339+ (January 2014) Tag fields such as those created by the Text Analytics module are identified with the tag icon.

Tip: In the Permissions and Fields tabs, you can type a string in a Filter box to easily refine the list to the elements containing the typed string. This feature is useful to quickly find a specific security entity or field in long lists.

6. In the information panel that appears, select the Summary tab to review a list of complete sentences recognized as important by an advanced linguistic algorithm.

Note: When no summary is displayed, summarization may have been disabled for this source to save CPU resources (see "Modifying General Source Parameters" on page 292).
8.7.1.2.4 Applying an Action on a Document From the Index Browser

From the Index Browser, you can easily apply an action to a unique indexed document (see "Index Browser Available Actions" on page 372). This feature is useful to independently treat an indexed document that requires maintenance.

**Example:** The director of a department of your organization identified an obsolete document that should no longer be found. You can locate the document and apply the **Remove from Index and Add Exclusion Filter** action on it.

To apply an action on a specific document from the Index Browser

1. In the Index Browser, locate the document on which you want to apply an action (see "Finding Documents Using the Index Browser" on page 374).
2. In the search results, click **Actions** below the search result for the document, and then select the desired action.

**Example:** Add the document **Modularization of XHTML** as a Top Result (see "Adding Top Results to a CES Index" on page 313).

**Note:** The list of available actions may vary depending on the type of source to which the document belongs.

8.7.1.2.5 Applying an Action on Multiple Documents From the Index Browser

From the Index Browser, you can easily apply an action on a set of indexed documents that you select individually or in lots from the search results (see "Index Browser Available Actions" on page 372). This feature is useful to independently treat sets of indexed documents that require maintenance.

To apply an action on multiple documents

1. In the Index Browser, locate the documents on which you want to apply an action (see "Finding Documents Using the Index Browser" on page 374).
2. Using the facets, ensure to select one collection and one source to activate the search results toolbar.
3. In the search results, select the check box of individual documents on which you want to perform an action.
4. Use the search results toolbar items shown in the following example to select, show, or clear selected
documents.

1. Select this check box to select all the documents listed in the current search results page (50 in the example).
2. Click to select all the documents returned by the current query (872 in the example).
3. Indicates the number of currently selected documents.
4. Click to show only the currently selected documents.
5. Click to clear all currently selected documents and start a new selection.
6. Select an action to apply to all the currently selected documents.

Note: You can perform several queries and select documents from any of them to build a precise set of selected documents.

5. When the currently selected documents are the ones on which you want to apply an action, on the search results toolbar, select the desired action to apply.
The action is performed, a confirmation message appears at the top of the page, and the document selection is cleared.

Notes:
- When adding Top Results, a dialog box appears to let you enter the queries (see "Adding Top Results from the Index Browser" on page 314).
- The list of available actions may vary depending on the type of sources to which the documents belong.

8.7.1.2.6 Applying an Action on Folders From the Index Browser

From the Index Browser, you can easily apply an action on all the documents contained in one or more folders from a given source (see "Index Browser Available Actions" on page 372). This feature is useful to independently treat sets of indexed documents that require maintenance.

Example: The director of a department of your organization identified an old folder in an indexed file share whose content should not be searchable as it is obsolete. You can locate and select the folder and apply the Remove from Index and Add Exclusion Filter action on it.

To apply an action on documents contained in one or more folders

1. On the Coveo server, access the Administration Tool.
2. In the Administration Tool, select Content > Index Browser.
3. In the Collection facet, select the collection that contains the folder(s) on which you want to apply an action.
4. In the Source facet that appears, select the source that contains the folder(s).
5. In the Folder facet that appears, select the check box for one or more folders containing documents to which you want to apply an action.
6. In the Folder Actions facet, select the action that you want to apply to all the documents contained in the currently selected folders.
8.7.1.3 Using the Security Browser

The Security Browser page allows you to look into the relationships between the indexed security user and groups found in your unified index. The features of this page are useful to troubleshoot indexing and search results issues involving security.

To use the Security Browser

1. On the Coveo server, access the Administration Tool.
2. In the Administration Tool, select Content > Security Browser.
3. In the Security Browser page:
a. In the Name box, enter the name of a user or group for which you want to browse the security.

Example: For an Active Directory user or group, enter the name in the domain\UserOrGroupName form such as MyOrg\JSmith.

Note: You must enter an exact case sensitive name. You cannot use wildcard.

b. In the second box on the same line, select the type or security entities for the typed name (User, Group, or Virtual Group).

Note: A Virtual Group is a group that is defined only in CES, not in a security provider.

c. In the third box on the same line, select the security provider in which the user or group is defined.

d. At the end of the same line, click View.

The page presents related security entities:

Navigation

Indicates the history of navigation among security entities. The last element is the current entity. Previous navigation elements are clickable to allow you to easily return to a previously selected security entity.

Members

Lists the security entities that are members of the currently selected security entity. The listed security entities are clickable so that you can easily explore the membership relationships.

Is Member of

Lists the security entities for which the currently security entity is a member. The listed security entities
are clickable so that you can easily explore the membership relationships.

e. To drill down in the security information, click a security entity in either the Members or the Is Member of list.

   The selected security item is added to the navigation history and the Members and Is Member of lists are updated.

f. Optionally, in the Filter box, type a string to refine the Members and Is Member of lists to only security entities that contain the typed string.

g. Optionally, in the Members or Is Member of lists:
   
   • Click the title of a column to sort the list alphabetically by the clicked column values. A second click sorts the values in the reverse order.
   
   • Click the funnel icon next to a column title and select the desired security entities to refine the list to these entities.

h. When you want to ensure that the CES security cache is up-to-date with the permissions associated with a given security group:

   i. In the Members or Is Member of list, click the group for which you want to update the permissions.

   ii. CES 7.0.6547+ (March 2014) At the bottom of the page, click the **Update permissions for: [group_name]** link.

      A message appears at the top of the page.
Note: The command to update permissions is sent immediately and executed as soon as previously committed operations are completed, typically within seconds.

Example: You just removed a member from a given Windows group and want to ensure in the Security Browser that the user no longer sees corresponding documents in the Coveo search results.

By default the Update Windows Users and Groups Cache system schedule is executed once a day at 12:00 AM (see “What Should Be the Frequency of System Schedules?” on page 442) so CES will normally be aware of the permission changes only at midnight.

You can use the Update permissions for: [group_name] link to force a security cache update for the specific group and continue your validation.

8.7.2 Administration Tool - Reports Tab

Reports are tools used to monitor the Coveo Platform. They provide charts and statistics to give a global overview of the index content and the processes recently performed on it.

CES can produce three types of reports: reports for queries (query history), for modifications brought to the index (index history) and for the index content (document statistics).

Note: Reports are limited to the content of the query and index history. To save disk space, query and index history are kept only for the time period specified in the Settings page (Reports > Settings)—by default, they are deleted after 15 days.

8.7.2.1 What Is the Difference between Reports and Logs?

Both reports and logs are monitoring tools for the Coveo Platform processes. However, reports provide general information in the form of charts and short statistic tables; whereas, logs provide written details for each event and process. Reports are used for quick troubleshooting when the cause of a problem is obvious, while logs allow the identification of system events that may not be immediately displayed.

Note: The Usage Analytics Module provides more tools to analyze the usage of your Coveo implementation (see "On-Premises Usage Analytics Module" on page 649).

8.7.2.2 What Information Is Displayed in the Query History?

The Query History page displays a chart and statistics concerning query results and the most common expressions queried during the specified time period. It is used to determine general trends in order to fine tune
search results and resolve search issues.

**Example:** If the expression Coveo AND help is often queried, it is possible to add the Coveo online help and other pertinent documents as Top Results.

**Notes:**

- The Usage Analytics Module provides more tools to analyze the usage of your Coveo implementation (see "On-Premises Usage Analytics Module" on page 649).

- Reports are limited to the content of the query and index history. To save disk space, query and index history are kept only for a configurable time period (see "Modifying the Report Settings" on page 391). By default, they are deleted after 15 days.
### Period
Displays charts and statistics for a **Fixed** (the last hour, 6 hours, week, etc.), **One month**, or a **Custom** time period (delimited by two dates).

### Chart
Displays the number of queries made during a specific time interval (ex.: between 9h00 and 9h30). The time intervals are dependent on the period selected (ex.: for a 1 day period, the time intervals are of 1 hour; whereas, for a 2 week period, the time intervals are of 1 day).

Point the cursor on a column to display statistics for this time interval.

### Query Statistics
Displays the number of queries made according to their result type as well as the maximum, minimum and average number of results per query.

There are four possible result types:
- **Successful**: The query returned at least one document.
- **No result**: The query did not return a document.
- **Corrected**: Users choose to apply a spelling correction proposed by CES.
- **Erroneous**: The query contained displayed one or several errors.

### Top Queries
Displays the most frequent query expressions according to their result type.

There are four result types:
- **Successful**: The query returned at least one document.
- **Erroneous**: The query contained displayed one or several errors.
- **No result**: The query did not return a document.
- **Corrected**: Users choose to apply a spelling correction proposed by CES.

### 8.7.2.3 What Information Is Displayed in the Index History?

The **Index History** page displays a chart and statistics about the documents subjected to indexing (including rejected documents). It is used to verify if the indexing process has encountered problems (ex.: CES was denied access to documents).

**Note**: Reports are limited to the content of the query and index history. To save disk space, query and index history are kept only for a configurable time period (see "Modifying the Report Settings" on page 391). By default, they are deleted after 15 days.

<table>
<thead>
<tr>
<th>Section</th>
<th>Description</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sources and Collections</td>
<td>Displays charts and statistics for the entire index or a single collection or source.</td>
<td>Select a collection or source to display, or display all the index content.</td>
</tr>
<tr>
<td>Period</td>
<td>Displays charts and statistics for a fixed time period (for example, the last hour, 6 hours, week, etc.) or a custom time period (delimited by two dates).</td>
<td>Select an option and a time interval to display in the chart and statistics.</td>
</tr>
<tr>
<td>Section</td>
<td>Description</td>
<td>Action</td>
</tr>
<tr>
<td>---------</td>
<td>-------------</td>
<td>--------</td>
</tr>
<tr>
<td><strong>View</strong></td>
<td>Displays documents encountered by the connector according to the type and subtype of action taken. There are three action types and nine subtypes:</td>
<td>Select the type of documents and information displayed.</td>
</tr>
<tr>
<td><strong>Indexed Documents:</strong></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
| - Added: New documents indexed. Documents previously indexed are listed as *Updated* when a source is refreshed or rebuilt.  
- Updated: Documents re-indexed.  
- Deleted: Documents removed from the index. |  |  |
| **Ignored Documents:** |  |  |
| - Filtered by source filters: Documents excluded by filters (see "Adding or Modifying Source Filters" on page 295).  
- Filtered by robot exclusion rules: Web documents excluded by robot exclusion (i.e. tags indicating that a site must not be crawled).  
- Filtered by document type: Documents excluded according to the document type set (see "What Are Document Type Sets?" on page 476).  
- Unchanged: Documents not modified since the last refresh (for refresh only, during rebuilds the documents are updated). |  |  |
| **Erroneous Documents:** |  |  |
| - Access denied: Documents for which CES does not have sufficient security permissions (see "Modifying the CES Log On Account" on page 227).  
- Not found: Web pages not found. |  |  |
| **Chart** | Displays the number of documents indexed, ignored or identified as erroneous during a specific time interval (ex.: between 9h00 and 9h30). Point the cursor on a column to display statistics for this time interval. | Point a column with the cursor to display the indexing statistics for this time interval. |
| **Document Statistics** | Displays the number of documents indexed, ignored or identified as erroneous during the time period. Details the action taken on indexed documents (added, updated, deleted) and justifies why other documents are rejected. | N/A |
| **Document Size Statistics** | Displays the total size of the document files indexed during the time period, as wells as the maximum, minimum and average document sizes. | N/A |
| **Note:** Document Size Statistics displays the file size—which is different from the document size in the index (the size of the document in the index is usually inferior to the file size because CES regroups data to save index space). |  |  |

### 8.7.2.4 What Information Is Displayed in the Document Statistics Page?

The **Document Statistics** page displays charts about the composition of the index (ex.: number of documents in a certain language, of a certain size). It is used to customize the search interface according to the index content.
Example: If the document statistics show that documents in several languages are indexed, it is useful to make the refine by language function available.

<table>
<thead>
<tr>
<th>Section</th>
<th>Description</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Topics</td>
<td>Displays charts about five possible subjects:</td>
<td>Select the charts to display.</td>
</tr>
<tr>
<td></td>
<td><strong>File types</strong>: The number of documents contained in the index for each</td>
<td></td>
</tr>
<tr>
<td></td>
<td>file type (ex.: HTML, XML, PDF)</td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Languages</strong>: The number of documents contained in the index for each</td>
<td></td>
</tr>
<tr>
<td></td>
<td>language recognized by CES.</td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Modified date</strong>: The number of documents contained in the index for</td>
<td></td>
</tr>
<tr>
<td></td>
<td>different modification dates (Today, This week, This month, This year</td>
<td></td>
</tr>
<tr>
<td></td>
<td>or in the Previous years).</td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Indexed date</strong>: The number of documents contained in the index for</td>
<td></td>
</tr>
<tr>
<td></td>
<td>different indexing dates (Today, This week, This month, This year and</td>
<td></td>
</tr>
<tr>
<td></td>
<td>in the Previous years).</td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>File size</strong>: The number of documents contained in the index for different</td>
<td></td>
</tr>
<tr>
<td></td>
<td>file sizes (less than 10 KB, Between 10 and 100 KB, Between 100 KB and 1 MB,</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Between 1 and 10 MB and More than 10 MB).</td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong>: The File size is different from the size of the document in the</td>
<td></td>
</tr>
<tr>
<td></td>
<td>index (the size of the document in the index is usually inferior to the</td>
<td></td>
</tr>
<tr>
<td></td>
<td>file size because CES regroups data to save index space).</td>
<td></td>
</tr>
</tbody>
</table>

| Collection and  | Displays charts for the entire index or for a single collection or source.  | Select a collection or source to display,  |
| Source          |                                                                            | or display all the index space.           |

| Charts           | Displays charts about the **Topics** selected.                             | Displays new statistics according to the   |
|                  |                                                                            | new topics and collection/source selected. |

8.7.2.5 Displaying Reports

Reports provide charts and statistics about queries (query history), modifications made to the index (index history) and index content (document statistics). The information displayed for each report can be customized.

**Note**: Reports are limited to the content of the query and index history. To save disk space, query and index history are kept only for a configurable time period (see "Modifying the Report Settings" on page 391). By default, they are deleted after 15 days.

To display a report

1. On the Coveo server, access the Administration Tool.
2. In the Administration Tool:
   - To display query history reports:
     a. Select **Reports > Query History**.
     b. In the **Query History** page, select the appropriate display options (see "What Information Is Displayed
To display index history reports:
   a. Select Reports > Index History.
   b. In the Index History page, select the appropriate display options (see "What Information Is Displayed in the Index History?" on page 388).
   c. Click Update.

To display document statistics reports:
   c. Click View Statistics.

8.7.2.6 Modifying the Report Settings

Report settings determine how large query and index history are kept in memory. By default, histories are kept for 15 days allowing to produce charts and statistics covering the two previous weeks (two weeks are usually enough to define general trends). Keeping histories for a longer time period allows to produce long term statistics but also requires more disk space.

To modify the report settings

1. On the Coveo server, access the Administration Tool.
2. In the Administration Tool, select Reports > Settings.
3. In the Settings page:
a. In the **Index History** and **Query History** sections, select the appropriate logging option.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Keep index/query history for the last X days</td>
<td>CES deletes histories after the specified number of days. For example, if histories are kept for 15 days, they are deleted on the 16th day.</td>
</tr>
<tr>
<td>Keep index/query history forever</td>
<td>CES does not delete histories unless the <strong>Delete index/query history older than</strong> option is used.</td>
</tr>
</tbody>
</table>
| Disabled | CES deletes all histories and does not register new ones. This option saves the most disk space, but disables an important monitoring tool.  
**Note:** No message is displayed in the **Query History** or **Index History** page to indicate that it is disabled. |
| Delete Index/Query History older than | CES deletes all histories registered before the specified date.  
**Example:** Delete index/query history older than 22 January 2012 deletes histories from January 21st 2012 and before. |

b. Optionally, enter the appropriate date in the **Delete index/query history older than** box and click **Delete index/query history older than** to save disk space.

c. In the **Top Query Count** box, enter the number of Top Queries that you want to see in the Queries History report.

d. Click **Apply Changes**.

### 8.7.2.7 Exporting Query/Index History in Excel Format

To save disk space, query and index history can be exported in Excel format—Excel files require 50% less disk space than the original history files.

**Tip:** After exporting histories, delete the original files (see "Modifying the Report Settings" on page 391).

To export query or index history in Excel format

1. On the Coveo server, access the Administration Tool.
2. In the Administration Tool, select **Reports > Query History** or **Reports > Index History**.
3. In the **Query History** or **Index History** page:
   a. Select the appropriate options (see "What Information Is Displayed in the Query History?" on page 386 or "What Information Is Displayed in the Index History?" on page 388).
   b. Click **Update**.
   c. Click **Export**.

Depending on your browser, the file is either immediately downloaded to your default download folder or a dialog box appears to allow you to select the folder where to save the file.
8.7.2.8 Why Is the Query/Index History Empty?

When the charts and statistics remain blank despite clicking **Update**, two things can be in cause:

- No querying or indexing action has occurred during the time period specified. Try modifying the time period or selecting a different collection or source. Remember, histories are deleted after the number of days (see "Modifying the Report Settings" on page 391).

- The recording of query or index history is disabled. Verify that they are not disabled (see "Modifying the Report Settings" on page 391).

**Note:** No message is displayed in the **Query History** or **Index History** page to indicate that it is disabled.

8.7.3 Administration Tool - Logs Tab

Logs are monitoring tools for the Coveo Platform. They detail individual events that have occurred during system tasks, queries or indexing operations. The log entries are similar to those of the CES Console. Though, logs keep track of past events; the CES Console provides real-time information (see "Using the CES Console" on page 246).

CES can produce three types of logs:

- Global logs about system operations (system log).
- Precise logs about the queries made (query log).
- Precise logs about the indexing process (index log).
- **CES 7.0.8225+ (March 2016)** Precise logs about the user actions in the Administration Tool (administration log).

**Note:** Before creating logs, it is preferable to adapt the log settings that determine the level of detail registered for each log.

8.7.3.1 What Information Is Displayed in the System Log?

The **System** page displays all events (including querying and indexing actions) that have occurred in the Coveo Platform during the specified time period. It is used to identify global errors and make sure the processes requested (ex.: source refresh, connection to a mirror server) have actually occurred.

The **System** page is made of two sections:

- The **Filters** section allows to choose what information is displayed in the logs.
- The **Logs** section displays the events in ascending or descending order.

**Note:** Before creating logs, it is preferable to adapt the log settings that determine the level of detail registered for each log and the time period during which logs are kept. By default, they are deleted after 90 days (see "Modifying the Log Settings" on page 402).
<table>
<thead>
<tr>
<th>Filter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Period</td>
<td>Displays the events that have occurred in a fixed time period (the last hour, 6 hours, week, etc.) or custom time period (delimited by two dates).</td>
</tr>
</tbody>
</table>
| Log Fields | Displays four types of information for each event:  
**Severity**: The severity of an event ranges from normal to critical. Normal events occur as part of CES processes; whereas, critical events indicate errors likely to cause a system failure. For more information concerning severity types, refer to the **Severity** filter section below.  
**Time**: The time (in hours, minutes, seconds) at which the event occurred.  
**Duration**: The number of seconds elapsed between the beginning and end of the event.  
**Description**: Information allowing to identify an event and the processes it is related to. |
| Severity | Displays four types of information for each event:  
**Details**: Precise information about normal events.  
**Information**: Generic information about normal events. This category is divided in two subcategories: **IMPORTANT** and **NORMAL.** System processes essential to CES functioning (ex.: starting the Coveo instance) are attributed **IMPORTANT** severity; whereas, non-essential processes (ex.: loading a source, enabling queries) are attributed **NORMAL** severity.  
**Warning**: Information about non-critical abnormal events. Non-critical events do not cause system failures.  
**Error**: Information about critical abnormal events. Critical abnormal events are likely to cause system failures.  
**Note**: By default, details are not displayed because they are not useful for troubleshooting (they describe events not essential to the system functioning) and create much longer logs. |
8.7.3.2 What Information Is Displayed in the Query Log?

The **Query** page displays detailed information concerning each query made (query expression, username, number of results, number of pages opened, etc.)—each query is a separate entry in the **Query** log. It is used to determine precisely what the user querying habits are in order to customize the Coveo Platform.

**Example:** If *Enterprise Search* is a frequent query that returns no result, it is possible to add synonyms for it in the thesaurus (ex.: associate it to CES) so that it returns pertinent documents.

The **Query** page is made of two sections:

- The **Filters** section allows to choose what information is displayed in the logs.
- The **Logs** section displays the events in ascending or descending order.

**Note:** Before creating logs, it is preferable to adapt the log settings that determine the level of detail registered for each log and the time period during which logs are kept. By default, they are deleted after 90 days (see "Modifying the Log Settings" on page 402).
### Queries Settings

<table>
<thead>
<tr>
<th>Filters</th>
<th>Logs</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Period</strong></td>
<td><strong>Logs</strong></td>
</tr>
<tr>
<td>Fixed One month Custom</td>
<td><strong>Sort:</strong> Descending <strong>View Log</strong></td>
</tr>
<tr>
<td>Length 6 hours</td>
<td><strong>Hide Filters Full Screen</strong></td>
</tr>
</tbody>
</table>

**Log Fields**
- Security
- Time
- Duration
- User
- IP address
- Query
- Advanced query
- Collections
- Corrected
- First result
- Requested results
- Returned results
- Filtered
- Sort by
- Status
- Error code
- Index
- Mirror
- Distributed
- Super User Access
- On behalf
- Full access from index browser

**Severity**
- Details
- Information
- Warning
- Error

**Query Status**
- Successful
- Errors
- Corrected
- No result
- Distributed
- Super User
- Full access from index browser

Select: All None

Click View Log to view the log entries.
### Filter | Description
--- | ---
**Period** | Displays the queries that have occurred in a fixed time period (the last hour, 6 hours, week, etc.) or custom time period (delimited by two dates).

**Mirror** | Displays the queries made on different mirror indexes.

**Note:** The query log can only be displayed for one mirror at a time.

**Log Fields** | Displays 18 types of information about each query:

**Severity:** The severity of an event ranges from normal to critical. Normal events occur as part of CES processes; whereas, critical events indicate errors likely to cause a system failure. *NORMAL* status is attributed to *Successful, No Result* and *Corrected* queries; whereas, erroneous queries are attributed a *WARNING*. For more information concerning severity types, refer to the **Severity** filter section below.

**Time:** The time (in hours, minutes, seconds) at which the query was sent.

**Duration:** The number of seconds CES took to perform the search.

**User:** The name of the user who sent the query. Usernames are registered only if, in the **Queries** section of the **Settings** page (**Logs > Settings**), the **Record the username and IP address for each query** check box is selected.

**IP address:** The IP address of the computer from which the query was sent. IP addresses are registered only if, in the **Queries** section of the **Settings** page (**Logs > Settings**), the **Record the username and IP address for each query** check box is selected.

**Query:** The expression queried.

**Advanced query:** The fields queried using the advanced search or the **Refine by** function of the result page.

**Collections:** The collections queried—if the search was restricted by collection using the advanced search.

**Corrected:** Whether a spelling correction was proposed for the query or not.

**First result:** The rank of the page opened—each page opened is a different log entry. The first page indicates 0, the second page indicates the number of results on the previous page (ex.: if the **Requested results** is 10, the second page displays 10), the third page displays the number of results on the two previous pages (ex.: if the **Requested results** is 10, the third page displays 20), and so on.

**Requested results:** The number of results per page requested by the user.

**Returned results:** The total number of results returned by the search.

**Filtered:** Whether duplicate documents are filtered or not.

**Sort by:** The parameter used to sort results.

**Status:** The type of query according to its results (Successful, Erroneous, No Result or Corrected).

**Error code:** The error code for *Erroneous* queries (usually **TOO_MANY_TERMS**). For Successful, No Result and Corrected, the error code is **SUCCESS**.

**Index:** The index on which the query is performed.

**Mirror:** The mirror on which the query is performed (which is the same as the **Mirror** filter selected).
### Filter | Description
--- | ---
**Severity** | Displays four types of information for each event:  
**Details:** Precise information about normal events.  
**Information:** Generic information about normal events. This category is divided in two subcategories: IMPORTANT and NORMAL. **Successful, No Results** and **Corrected** queries are attributed NORMAL severity. **IMPORTANT** severity identifies essential system processes (ex.: starting the Coveo instance), thus it is not used for queries.  
**Warning:** Information about non-critical abnormal event. **Erroneous** queries are attributed a WARNING.  
**Error:** Information about critical abnormal events. Critical abnormal events are likely to cause system failures.  
**Note:** By default, details are not displayed because they are not useful for troubleshooting (they describe events not essential to the system functioning) and because they create much longer logs.

**Query Status** | Determines which queries are displayed in the logs according to their status.  
**Successful:** The query returned at least one document.  
**Erroneous:** The query contained too many terms and was truncated—the maximum number of terms per query is specified in the Advanced page.  
**No result:** The query did not return any document.  
**Corrected:** Users choose to apply a spelling correction proposed by CES.

**Super User Access** | Determines which queries are displayed when you enter a super user token in the text box. You can find the existing super user token in the ID column from the Super User Access page (see "Managing Super User Access" on page 423). Leave the text box empty to view all queries performed with all super user tokens.  
In the logs, the **Super User Access** column indicates the super user token used, the **On behalf browser** column indicates if the query was performed in the Index Browser.

### 8.7.3.3 What Information Is Displayed in the Index Log?

The **Index** page displays detailed information concerning each indexing action (documents filtered, files not found, etc.). It is used to identify indexing errors and make sure all the repositories have been properly rebuilt or refreshed.

**Example:** It is possible to identify the complete path and filename of documents that have been rejected during indexing.

The **Index** page is made of two sections:

- The **Filters** section allows to choose what information is displayed in the logs.
- The **Logs** section displays the events in ascending or descending order.

**Note:** Before creating logs, it is preferable to adapt the log settings that determine the level of detail registered for each log and the time period during which logs are kept. By default, they are deleted after 90 days (see "Modifying the Log Settings" on page 402).
The image displays a page from the Coveo Platform 7.0 Administrator Guide. The page shows a screenshot of the Logs section, which is used to manage indexing operations. The Logs section includes options for filtering and viewing the log entries. Filters can be applied based on various criteria such as severity, index, and source. The page also includes a link to www.coveo.com.
<table>
<thead>
<tr>
<th>Filter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Period</td>
<td>Displays the events that have occurred in a fixed time period (the last hour, 6 hours, week, etc.) or custom time period (delimited by two dates).</td>
</tr>
<tr>
<td>Log Fields</td>
<td>Displays 14 types of information concerning each event:</td>
</tr>
<tr>
<td></td>
<td><strong>Severity</strong>: The severity of an event ranges from normal to critical. Normal events occur as part of the Coveo processes; whereas, critical events indicate errors likely to cause a system failure. The <strong>NORMAL</strong> status is attributed to all indexing processes; whereas, pages and documents not found are attributed a <strong>WARNING</strong>. For more information concerning severity types, refer to the <strong>Severity</strong> section below.</td>
</tr>
<tr>
<td></td>
<td><strong>Time</strong>: The time (in hours, minutes, seconds) at which the indexing action was started.</td>
</tr>
<tr>
<td></td>
<td><strong>Duration</strong>: The number of seconds CES took to crawl and convert (or reject) the document.</td>
</tr>
<tr>
<td></td>
<td><strong>Description</strong>: Information allowing to identify the indexing action.</td>
</tr>
<tr>
<td></td>
<td><strong>Address</strong>: The path of the document subjected to indexing.</td>
</tr>
<tr>
<td></td>
<td><strong>Indexing operation</strong>: The action taken on the document (ex.: Updated, Not Found, Filtered). For more information concerning operations, refer to the <strong>Index Operations</strong> filter section below.</td>
</tr>
<tr>
<td></td>
<td><strong>Collection</strong>: The collection (i.e. group of repositories) of the document (even rejected documents are attributed a collection).</td>
</tr>
<tr>
<td>Language</td>
<td>The languages identified by CES for the document.</td>
</tr>
<tr>
<td>Format</td>
<td>The file type of the document.</td>
</tr>
<tr>
<td>Size</td>
<td>The size, in bytes, of the document file.</td>
</tr>
<tr>
<td>Note</td>
<td>The size of the document in the index is usually inferior to the size of the document file because CES regroups data to save index space.</td>
</tr>
<tr>
<td>Source</td>
<td>The repository of the document (even rejected documents are attributed a source).</td>
</tr>
<tr>
<td>Status</td>
<td>Whether the indexing process was successful (a failure indicates a problem connecting to the repository or a system error).</td>
</tr>
<tr>
<td>Links</td>
<td>The number of links encountered by the connector in the document.</td>
</tr>
<tr>
<td>Broken link</td>
<td>The number of broken links encountered by the connector in the document.</td>
</tr>
<tr>
<td>Severity</td>
<td>Displays 4 types of information for each event:</td>
</tr>
<tr>
<td>Details</td>
<td>Precise information about normal events.</td>
</tr>
<tr>
<td>Information</td>
<td>Generic information about normal events. This category is divided in two subcategories: <strong>IMPORTANT</strong> and <strong>NORMAL</strong>. Documents Added, Updated, Filtered and Deleted are attributed <strong>NORMAL</strong> severity. <strong>IMPORTANT</strong> severity identifies essential system processes (ex.: starting the Coveo instance), thus it is not used for indexing actions.</td>
</tr>
<tr>
<td>Warning</td>
<td>Information about non-critical abnormal event. Files <strong>Not Found</strong> are attributed a <strong>WARNING</strong>.</td>
</tr>
<tr>
<td>Error</td>
<td>Information about critical abnormal events. Critical abnormal events are likely to cause system failures.</td>
</tr>
<tr>
<td>Note</td>
<td>By default, details are not displayed because they are not useful for troubleshooting (they describe events not essential to the system functioning) and because they create longer logs.</td>
</tr>
<tr>
<td>Collection and Source</td>
<td>Displays the logs for the entire index or for a specific collection or source.</td>
</tr>
</tbody>
</table>
### Filter Operations

<table>
<thead>
<tr>
<th>Filter Operations</th>
<th>Description</th>
</tr>
</thead>
</table>
| Determines which operations are displayed in the logs. There are 10 operations:  
**Added**: The document was added to the index for the first time (documents previously indexed are identified as *Updated* even during a rebuild).  
**Deleted**: The document is removed from the index.  
**Updated**: A more recent version of the document is indexed.  
**Unchanged**: During the refresh, the document is not updated because it has not been modified since the last indexing. (During a rebuild, the document is updated).  
**Filtered by document type**: The document is not indexed or removed from the index because the action for its document type is *Reject document*.  
**Unauthorized**: The connector does not have sufficient permissions to open the document—thus, it is not indexed.  
**Not found**: The Web page on which the document is located was not found.  
**Filtered by source filters**: The document is not indexed or removed from the index by an exclusion filter.  
**Filtered by robot exclusion rules**: The connector could not index the Web page because of a robot exclusion rule (i.e. tags indicating that a site must not be crawled).  
**No operation**: No operation is attempted on the document. |

### 8.7.3.4 Displaying Logs

Logs provide details about events that have occurred during system tasks (system log), queries (queries log) or indexing operations (index log). The log entries are similar to those of the CES Console. Though, logs keep track of past events; whereas, the CES Console provides real-time information (see "Using the CES Console" on page 246).

**Note**: Before creating logs, it is preferable to adapt the log settings that determine the level of detail registered for each log and the time period during which logs are kept. By default, they are deleted after 90 days (see "Modifying the Log Settings" on page 402).

To create a log

1. On the Coveo server, access the Administration Tool.

2. In the Administration Tool:
   - To display query history reports:
     a. Select **Logs > System**.
     b. In the **System** page, select the information to display (see "What Information Is Displayed in the System Log?" on page 393).
     c. Click **View Log**.
   - To display index history reports:
8.7.3.5 Modifying the Log Settings

Log settings determine the level of details registered for each log and the time period during which logs are kept. By default, they are deleted after 90 days. Three months is usually enough to identify and correct system errors.

When logs cannot be fully analyzed over the three month period, it is suggested to keep them longer to avoid losing track of unnoticed errors—allow sufficient index space (30 days of logs require at least 10 megabytes and can reach a few hundred megabytes depending on the number of entries and the level of detail registered).

To modify the log settings

1. On the Coveo server, access the Administration Tool.
2. Access the Settings page (Logs > Settings).
3. In the Settings page:
a. In the **Queries** section:

   i. Select the **Enable query logging** check box to start logging query information.

   When query logging is disabled, new queries are not registered. However, previous query logs are not deleted. All logs are deleted at the same time, after the specified number of days.

   ii. Select the **Record the username and IP address for each query** to help you identify who is using your Coveo search interfaces. Allow sufficient disk space for the additional data.

   **Note:** When hundreds of users are querying the CES7 index on a regular basis, query logging requires a few hundred megabytes of disk space for each 30-day period.

b. In the **Index Log Level** section, select the level of detail to register for the index log:

   - **Detailed Information:** Registers all events disregarding their severity.
   - **Information:** Does not register details.
   - **Warnings and Errors:** Does not register information or details.
   - **Errors Only:** Registers only critical errors (i.e. errors likely to cause a system failure).

   **Note:** The actual level of detail displayed in the logs depends on the **Severity** filter. However, log entries can only be displayed for registered events. For example, if **Errors Only** is selected, it is impossible to display warnings, information or details.

c. In the **Query Log Level** section, select the level of detail to register for the queries log.

d. In the **Index Log Archive** and **Query Log Archive** sections, select the number of days for which the logs are kept, or to keep all logs.

e. Click **Apply Changes**.
8.7.3.6 Why Is the Query and Index Log Empty?

If the query/index log remains blank despite clicking View Log, two things can be in cause:

- **For query and index logs**: No querying or indexing action has occurred during the specified time period. Try modifying the period. Remember that logs are deleted after the number of days (see "Modifying the Log Settings" on page 402).

- **For query log**: Query logging is disabled. Enable logs (see "Modifying the Log Settings" on page 402).

8.7.3.7 Reviewing Administration Changes

The **Administration Logs** page displays all operations in the Administration Tool that were triggered by a user interaction. Every performed event appears within seconds in the logs, meaning the page can be used to monitor the Administration Tool.

This page is also useful to help solving support cases by providing relevant information such as the owner of each source and the user responsible for errors or unauthorized content permission changes.

To review administration changes

1. On the Coveo server, access the Administration Tool.

2. Select Logs > Administration.

3. In the Administration Logs page, you can:

   ![Example of Administration Logs page](image-url)
Select the period for which you want to review user actions in the Administration Tool:

a. In the filter toolbar, next to From or To, click the calendar icon.

b. In the calendar picker that appears, use the left and right arrows icons to reach the desired month, and select the date from or to which you want to review operations.

c. Repeat the process for the other calendar icon.

Filter user operations to only review those you want

a. In the filter toolbar, click the Filter box.

b. Enter the value you want to filter on, and then press Enter.

Note: Except dates, which are delimited using the calendar pickers, every text value contained in the logs can be filtered on.

Sort user actions

Click the column header titles to sort the user actions by Page, Action, Values, User, and Date. If the list is already sorted by the selected column header, the sort will change from ascending to descending or vice versa.

Review user operations

For each operation, you have the following information:

Note: Column values are displayed in a user-friendly manner to clearly show before and after values following changes. Most of the time, you will be familiar with the logged values since they reflect parameters, pages, names and labels that appear in the Administration Tool interface, facilitating the understanding of the logs.

- The Administration Tool page in which the operation occurs.
- The precise operation (e.g., Delete source [name]).
- Details of the operation [e.g., source parameter (before and after) values]

Notes:
- All form field values are compared before and after a user performs an action in the Administration Tool, and only the modified values are logged. In the logs, original values are crossed-out.
- Passwords are hashed for obvious security reasons.
- The user that performed the action (e.g., [DOMAIN]\[username])
- The time and day of the action in the Windows configuration panel format.

8.7.4 Administration Tool - Configuration Tab

This section regroups topics that help you, among other things, to configure the CES security parameters, create source refresh schedules, and enter new Coveo Enterprise Search (CES) license codes.
8.7.4.1 Administration Tool - Security Menu

Use this menu to configure all security aspects surrounding connectors and sources content permissions.

**Note:** Other security related topics not linked to the Administration Tool are available (see "Security" on page 218).

8.7.4.1.1 About Administration Roles

In an organization using the Coveo Platform, one or more persons may need to access the Coveo Web tools (Administration Tool, Interface Editor) to configure and manage various aspects of the Coveo solution. The Coveo Platform includes administration roles that allow to securely manage who has access to which features from the Coveo Web tools (see "Assigning Users to Administration Roles" on page 412).

**Notes:**

- When a member of an administration role has partial access to the Coveo Administration Tool, the features to which access is restricted (tabs, menus, parameters...) are visible but disabled, appearing shaded.
- When you add a local Windows administrator account while CES is running, CES does not automatically become aware of the existence of the new account.

Depending on your CES version, allow access to this new user:

- **CES 7.0.6607+ (April 2014)** You can manually refresh the CES security cache.
- **CES 7.0.6547– (March 2014)** You must restart the CES service.

**Important:** A user having administrator permissions on the Coveo server automatically gets the equivalent of the System Administrator (Limited Access) role. The administration roles apply to web connections to the Coveo Administration Tool and Interface Editor.

8.7.4.1.1.1 Administration Role Feature Comparison

The following tables respectively provide a comparative list of operation and configuration available to each administration role.

<table>
<thead>
<tr>
<th>Operation</th>
<th>System Admin. (Full)</th>
<th>System Admin. (Limited)</th>
<th>Index Admin. (Full)</th>
<th>Index Admin. (Limited)</th>
<th>Relevance Analysts</th>
<th>&quot;Search Interface Designer&quot; on page 412</th>
<th>Usage Analysts</th>
<th>Index Browser (Full)</th>
<th>Index Browser (Limited)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Change license</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Enable read-only</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Control remote mirrors</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Operation</td>
<td>System Admin. (Full)</td>
<td>System Admin. (Limited)</td>
<td>Index Admin. (Full)</td>
<td>Index Admin. (Limited)</td>
<td>Relevance Analysts</td>
<td>Usage Analysts</td>
<td>Index Browser (Full)</td>
<td>Index Browser (Limited)</td>
<td></td>
</tr>
<tr>
<td>-----------------------------------------------</td>
<td>----------------------</td>
<td>-------------------------</td>
<td>---------------------</td>
<td>------------------------</td>
<td>--------------------</td>
<td>-----------------</td>
<td>----------------------</td>
<td>-------------------------</td>
<td></td>
</tr>
<tr>
<td>Delete index content</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Delete old logs</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Access Usage Analytics module</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Display top queries</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>View query logs</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>View system logs</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>View index logs</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Rebuild sources</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Refresh/increment sources</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Pause/resume sources</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Refresh/remove documents</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Refresh converter scripts</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Test converters</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Commit current transactions</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Clean GroupBy cache</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Refresh security cache</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Browse index</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Browse index without checking permissions</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>✓</td>
<td></td>
</tr>
</tbody>
</table>
## Operation

<table>
<thead>
<tr>
<th>Operation</th>
<th>Administration roles</th>
</tr>
</thead>
<tbody>
<tr>
<td>System Admin. (Full)</td>
<td>✓</td>
</tr>
<tr>
<td>System Admin. (Limited)</td>
<td>✓</td>
</tr>
<tr>
<td>Index Admin. (Full)</td>
<td>✓</td>
</tr>
<tr>
<td>Index Admin. (Limited)</td>
<td>✓</td>
</tr>
<tr>
<td>Relevance Analysts</td>
<td>✓</td>
</tr>
<tr>
<td>Usage Analysts</td>
<td>✓</td>
</tr>
<tr>
<td>Index Browser (Full)</td>
<td>✓</td>
</tr>
<tr>
<td>Index Browser (Limited)</td>
<td>✓</td>
</tr>
</tbody>
</table>

- Modifications through Web services ✓

## Configuration

<table>
<thead>
<tr>
<th>Configuration</th>
<th>Administration roles</th>
</tr>
</thead>
<tbody>
<tr>
<td>System</td>
<td>✓</td>
</tr>
<tr>
<td>System/transaction update frequency</td>
<td>✓ ✓ ✓</td>
</tr>
<tr>
<td>System performance cache memory</td>
<td>✓ ✓ ✓</td>
</tr>
<tr>
<td>System performance mode</td>
<td>✓ ✓ ✓</td>
</tr>
<tr>
<td>Log</td>
<td>✓</td>
</tr>
<tr>
<td>Mail alert</td>
<td>✓</td>
</tr>
<tr>
<td>Mirrors</td>
<td>✓</td>
</tr>
<tr>
<td>Slices</td>
<td>✓</td>
</tr>
<tr>
<td>Remote indexes</td>
<td>✓</td>
</tr>
<tr>
<td>Administration roles</td>
<td>✓</td>
</tr>
<tr>
<td>Super user tokens</td>
<td>✓</td>
</tr>
<tr>
<td>Search pages to keep hot</td>
<td>✓</td>
</tr>
<tr>
<td>Crawlers/top queries count</td>
<td>✓</td>
</tr>
</tbody>
</table>

- System/transaction update frequency ✓ ✓ ✓  
- System performance cache memory ✓ ✓ ✓  
- System performance mode ✓ ✓ ✓  
- Log ✓  
- Mail alert ✓  
- Mirrors ✓  
- Slices ✓  
- Remote indexes ✓  
- Administration roles ✓  
- Super user tokens ✓  
- Search pages to keep hot ✓  
- Crawlers/top queries count ✓  

[408 www.coveo.com]
<table>
<thead>
<tr>
<th>Configuration</th>
<th>System Admin. (Full)</th>
<th>System Admin. (Limited)</th>
<th>Index Admin. (Full)</th>
<th>Index Admin. (Limited)</th>
<th>Relevance Analysts</th>
<th>Usage Analysts</th>
<th>Index Browser (Full)</th>
<th>Index Browser (Limited)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Crawlers/crawling paused</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Crawlers/live history size</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Collections/add</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Collections/remove</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Sources/add</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Sources/remove</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Source/schedule</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Source/filters</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Source/fields</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Source/XML definition</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Source/document type</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Source/Crawler source parameters</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Source/language</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Source/scripts</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Converter scripts</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Converters</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Language hint</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Schedules</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Security providers</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Document types</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Field aliases</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
## Administration Roles

<table>
<thead>
<tr>
<th>Configuration</th>
<th>System Admin. (Full)</th>
<th>System Admin. (Limited)</th>
<th>Index Admin. (Full)</th>
<th>Index Admin. (Limited)</th>
<th>Relevance Analysts</th>
<th>&quot;Search Interface Designer&quot; on page 412</th>
<th>Usage Analysts</th>
<th>Index Browser (Full)</th>
<th>Index Browser (Limited)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fields</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>XML document definitions</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SharePoint references</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>User identities</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Top Results</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>✓</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Ranking</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>✓</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Result clustering</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>✓</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Collaborative ranking</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>✓</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Thesaurus</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>✓</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Search interfaces</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>✓</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Search hubs</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>✓</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Search data</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>✓</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### 8.7.4.1.1.2 Administration Role Short Descriptions

**Administration role name format** is `[Role]([Permissions|Collections])`.  

When you add a role in the **Configuration > Security > Roles > Assign administration roles** page, you make a selection in the **Roles** and **Permissions** or **Collections** lists.
Example: When you want to give a user the **System Administrator (Full Access)** role, you first select **System Administrator**, and then select **Full Access** under **Index Browser** in the **Permissions** box that appears.

**System Administrator (Full Access)**

Members of this role have the same access as the System Administrators (Limited Access) role but also full read access to document details for all indexed documents, like for the Index Browsers (Full Access) role. This role is typically assigned to IT persons who need to review details from all indexes documents to be able to troubleshoot Coveo Platform issues.

**Important:** Members of the System Administrators (Full Access) role can see potentially sensitive information such as document titles, document summaries, metadata values. This role provides Super User-like access but index browser queries made with this role are logged so that they become traceable. Assign this role with care.

**System Administrator (Limited Access)**

Members of this role have access to all Coveo Web tool features, including read access to index browser document details but only for documents that they normally have access, like for the Index Browsers (Limited Access) role. For other documents, inaccessible to the member, document details are hidden, protecting potentially sensitive information. A number of features are exclusive to this role, including assigning other users to administration roles (see "Assigning Users to Administration Roles" on page 412). This role is typically assigned to IT persons in charge of the Coveo solution.

**Relevance Analyst**

Members of this role have access to Top Results (for all collections and sources), ranking, clustering, and thesaurus configuration to control how the index content is returned for end-user queries. This role is typically assigned to persons in charge of ensuring search users can easily find documents they are looking for.
Usage Analyst

Members of this role have access to query logs/history and the Usage Analytics module to analyze how the Coveo solution is used. This role is typically assigned to persons in charge of evaluating the adoption of the Coveo solution, such as the project manager or the solution owner.

Important: Usage Analysts gain full access to the Usage Analytics module interface where potentially sensitive information can be exposed as all queries by all users can be viewed. Assign this role with care.

Index Administrator (Full Access)

Members of this role have access to all index operation and configuration for all collections and sources, but do not have access to the index browser. They can change configuration affecting many or all collections and sources. This role is typically assigned to IT persons in charge of the Coveo solution.

Index Administrator (Limited Access)

Members of this role have access to basic index operation and configuration for selected collections and sources. Users member of this role cannot change configuration affecting more than one collection or sources. This role can be assigned to persons in charge of specific indexed repositories to give them access to basic index operation and configuration for the corresponding collections and sources.

Index Browser (Full Access)

Members of this role have access to the index browser with read access to document details for all indexed documents. Access to this information is useful when required to see what documents and metadata are available in the index while attempting to troubleshoot unexpected behavior of the Coveo Platform. This role is typically assigned to IT persons or information managers who need to review details from all indexed documents to be able to troubleshoot Coveo Platform issues.

Important: Members of the Index Browser (Full Access) role can see potentially sensitive information such as document titles, document summaries, metadata values. This role provides Super User-like access but index browser queries made with this role are logged so that they become traceable. Assign this role with care.

Index Browser (Limited Access)

Members of this role have read access to index browser document details but only for documents this user has normally access to. For other documents, inaccessible to the current user, document details are hidden, protecting potentially sensitive information. This role is typically assigned to IT persons or information managers in charge of troubleshooting Coveo Platform issues.

Search Interface Designer

Members of this role have access to the Interface Editor where out-of-the-box search hubs and search interfaces can be customized, as well as new ones created and configured. This role is typically assigned to IT persons in charge of the search interfaces for the Coveo Platform.

8.7.4.1.2 Assigning Users to Administration Roles

If you can connect to the Coveo server or if you are a member of the System Administrators, you can assign users or groups to at least one of the available administration roles (see "About Administration Roles" on page 406). These
users or groups can then securely access the Administration Tool and Interface Editor features specifically associated with their administration role membership.

To assign users to administration roles

1. On the Coveo server, access the Administration Tool.
3. In the navigation panel that appears on the left, click Roles.
4. In the panel on the right, click Add to assign an administration role.

Note: You can also click an existing name to modify its administration roles, or click the delete icon ( ) next to the name to completely delete the assigned administration role.

5. In the Assign Administration Roles page:
a. Using the Security Provider, Type, and Name parameters, specify the user or group that you want to assign to an administration role.

   **Note:** For Active Directory security providers, enter the Name in the domain\user or domain\group form.

b. In the Roles panel, select the role to which you want to assign the user or group (see "About Administration Roles" on page 406).

   - When you select System Administrator, in the Permissions box that appears on the right, under Index Browser, select Full Access or Limited Access.

   **Note:** CES 7.0.7104–(October 2014) When you select System Administrator, in the Index Browser Roles Types box that appears, select Full Access or Limited Access.

   - When you select Partial Permissions, you can select one or more of the following roles:
     - Relevancy Analysts
     - Usage Analysts

   - When you select Index Administrators, in the Collections box that appears on the right, you can also select Full Control or limited control for All Collections or for a Subset of collections. When you select collections containing more than one source, in the Sources box that appears, you can
also select limited control for **All Sources** or for a **Subset** of the sources from the selected collections.

- When you select **Index Browser**, in the Permissions box that appears, under **Index Browser**, select **Full Access** or **Limited Access**.

**Note:** CES 7.0.7104–(October 2014) When you select **Index Browser**, in the **Index Browser Roles Types** box that appears, select **Full Access** or **Limited Access**.

- **Search Interface Designer**
  
  c. Click **Save** when creating a new set, or **Apply changes** when modifying an existing set.

### 8.7.4.1.3 What Is an Impersonator?

An impersonator is an account which uses the security permissions of another account in order to gain access to restricted documents. In the Coveo Platform, impersonation is used as a way to gain remote access to collections—especially in front-end/back-end configurations (where the search interface and index are located on different servers) because Windows does not allow a security token (object containing the user permissions) to be transmitted over the network twice (double-hop).

**Example:** Using impersonation in a front-end/back-end network configuration.

The user connects to one of the front-end servers (containing the search interface) via the intranet in order to query the back-end server (containing the index). If impersonation is not configured, the user security token is transmitted to the front-end server but cannot be retransmitted to the back-end server, because Windows prevents this double-hop. Therefore, the index cannot verify the user permissions and returns only documents available to everyone. However, if the front-end server has impersonator privileges, no token is exchanged between the user and server; instead, the front-end server assumes the identity of the user and sends the token directly to the back-end server—which returns all documents the user is allowed to open.

To allow impersonation, the front-end server address must be entered in the **Impersonators** list (see "Granting Impersonator Privileges" on page 415).

### 8.7.4.1.4 Granting Impersonator Privileges

In CES, impersonation is used as a way to allow remote Front-End applications to gain access to collections.

**Example:** When the search interfaces and the index are located on different servers, the Back-End server must be configured to accept queries from the Front-End servers. On each Coveo Master server, this is done by adding an impersonator for the identity running the AppPool of the remote process for each Front-End server.

To grant impersonator privileges to an account

1. On the Back-End server, open the Administration Tool (Windows Start menu > **All Programs** > **Coveo Enterprise Search 7** > **Administration Tool**).
2. In the Administration Tool, select **Configuration** > **Security**.
3. In the navigation panel on the left, click **Impersonators**.
4. In the **Impersonators** page:
a. Click **Add**.

b. In the **Add Identity** dialog box, specify the user to which you want to grant impersonation privileges (see "Using the Identity Picker Form" on page 428).

c. Click **Add**.

The account name is added to the list of impersonators.

**Notes:**

- In the **Name** box, enter the account in the `domain\username` form for the Coveo instance (Front-End server) from which you want to access this index for both:
  - The account running the CES Service (see "About the CES Service Logon Account" on page 225).
  - The account running the CES search application (CESAppPool in IIS) (see "Finding or Modifying the CES Search Application Pool Identity" on page 79).

- When the account used is `NT AUTHORITY\NETWORK SERVICE`, enter the account name in the form `domain\MachineName$` where `MachineName` is the name of the server from which you send queries (Front-End server).
What's Next?

On your Front-End server(s), in the Coveo .NET Front-End web.config file, add the `impersonate="true"` attribute to the `<server hostname="localhost" port="52800" enable65SearchAPI="true" impersonate="true"/>` line to complete the impersonation configuration.

8.7.4.1.5 What Are Security Providers?

Coveo Enterprise Search (CES) supports indexing the content and security permissions of several repositories such as Active Directory, Microsoft SharePoint, Microsoft Exchange, Sitecore, Salesforce, and many more.

CES handles security permissions largely using security providers that act as bridges between the security model of each external system and the way permissions are represented in the Coveo index.

CES authenticates itself on the repositories using the parameters of each security provider, retrieves all accounts (users and groups), expands groups, establishes mappings between the various accounts of a user in different repositories, and stores this information in the Security Cache (see "What Is a Security Cache?" on page 264). Once mappings have been created for all security providers, CES is able to respect the native document permissions, returning in search results only documents a user is allowed to see.

A Coveo search interface can also use security providers to allow users to log in and validate their credentials for specific repositories.

8.7.4.1.6 Adding or Modifying a Security Provider

Security providers are authentication systems used by various systems. The security provider for Windows is Active Directory. Coveo Enterprise Search (CES) comes with three security providers by default (Active Directory, Custom and SharePoint). When your Coveo instance indexes repository types that use other security provider types and want to index their document security, you must configure a security provider for each repository type.

To add or modify a security provider

1. On the Coveo server, access the Administration Tool.
2. In the Administration Tool, select Configuration > Security.
3. In the navigation panel on the left, click Security Providers.
4. In the Security Providers page:
To create a new security provider, click Add.

To modify an existing security provider, in the Security Providers list, click the security provider that you want to modify.

5. In the Modify Security Provider page, the parameters that appear change depending on the Security Provider Type that you select.

Refer to the documentation of the appropriate connector for details (see "Coveo Platform Connectors" on page 734).

8.7.4.1.7 Restarting a Security Provider

You may encounter situations where a security provider is in error even when its configuration is valid. In this case, you can fix the condition and manually restart the security provider.

Examples:

- When a security provider starts, and the system for which it provides security is down, the security provider may become in error. You can start the system, and restart the security provider.

- When using a custom security provider, its DLL file may not be present in the appropriate folder when you attempt to start the security provider. Ensure the DLL file is copied to the folder and restart the security provider.

To restart a security provider

1. On the Coveo server, access the Administration Tool.

2. In the Administration Tool, select Configuration > Security.

3. In the navigation panel on the left, click Security Providers.
4. In the **Security Providers** page:

![Security Providers page](image.png)

- Select the check box of one or more security provider that you want to restart.
- **CES 7.0.5388+ (April 2013)** Click **Restart**.

---

**Note:** CES 7.0.5031– (March 2013) You need to modify a security provider and click **Save** to restart it (see “Adding or Modifying a Security Provider” on page 417).

### 8.7.4.1.8 Restarting a Security Provider

You may encounter situations where a security provider is in error even when its configuration is valid. In this case, you can fix the condition and manually restart the security provider.

#### Examples:

- When a security provider starts, and the system for which it provides security is down, the security provider may become in error. You can start the system, and restart the security provider.

- When using a custom security provider, its DLL file may not be present in the appropriate folder when you attempt to start the security provider. Ensure the DLL file is copied to the folder and restart the security provider.

To restart a security provider:

1. On the Coveo server, access the Administration Tool.
2. In the Administration Tool, select **Configuration > Security**.
3. In the navigation panel on the left, click **Security Providers**.
4. In the **Security Providers** page:
8.7.4.1.9 Adding a User Identity

A user identity is a set of credentials for a given repository or system that you enter once in CES and can then associate with one or more sources or security providers.

A user identity typically holds the credentials of an account that has read access to all the repository items that you want to index. It is a best practice to create an account to be used exclusively by the Coveo processes and for which the password does not change. If the password of this account changes in the repository, you must also change it in the CES user identity.

To add a user identity

1. On the Coveo server, access the Administration Tool.
2. In the Administration Tool, select Configuration > Security.
3. In the navigation panel on the left, click User Identities.
4. In the User Identities page, click Add.
5. In the Modify User Identity page:
a. In the Name box, enter a name of your choice to describe the account that you selected or created in the repository to allow CES to access the repository.

**Note:** This name appears only in the Coveo Administration Tool, in the Authentication or User Identity drop-down lists, when you respectively define a source or a security provider.

b. In the User box, enter the username for the account that you selected or created to crawl the repository content that you want to index.

c. In the Password box, enter the password for the account.

d. In the Options section, the Support basic authentication check box is deprecated and not applicable for most types of repositories. You should select it only when you need to allow CES to send the username and password as unencrypted text.

e. Click Save.

**Important:** When you use Firefox to access the Administration Tool and it proposes to remember the password for the user identity that you just created, select to never remember the password for this site to prevent issues with automatic filling of username and password fields within the Coveo Administration Tool.

### 8.7.4.1.10 Exporting/Importing User Identities

You can define user identities and then export them to an XML file. This allows you to easily import user identities in CES on another Coveo server. The export process encrypts passwords to provide a secure migration.

**Example:** The export/import user identity feature is useful to simplify the migration of user identity information between your Coveo instances in your development, QA, and production environments.

**Note:** To prevent losing user identity information, the import process fails when the exported XML file contains a user identity with a name identical to one on the target Coveo server.
To export and import user identities

1. **On the source Coveo Master server:**
   a. Access the Administration Tool (see "Opening the Administration Tool" on page 256).
   b. In the Administration Tool, select **Configuration > Security**.
   c. In the navigation panel on the left, select **User Identities**.
   d. Under **User Identities**, select one or more user identities that you want to export.
   e. Click **Export**.
      
      Save the **UserIdentityExport.xml** file to a folder of your choice.
   f. Using a text editor, open the XML file, and copy the content of the file.

   **Note:** You can also manually create a user identity XML file (see "User Identity XML File Format" on page 422).

2. **On the target Coveo Master server:**
   a. Access the Administration Tool (see "Opening the Administration Tool" on page 256).
   b. In the Administration Tool, select **Configuration > Security**.
   c. In the navigation panel on the left, select **User Identities**.
   d. Click **Import**.
   e. In the **Import User Identities** page that appears, paste the content of the **UserIdentityExport.xml** file that you want to import in the **Exported user identities list XML file content** box.
   f. Click **Apply Changes** to import the user identities.

**8.7.4.1.10.1 User Identity XML File Format**

This topic describes the format of the XML file generated when you export user identities (see "Exporting/Importing User Identities" on page 421). You can also manually create a user identity XML file using the syntax illustrated in the following example and XML element definitions.
Example: The following XML file contains two user identities.

```xml
<?xml version="1.0" encoding="UTF-8"?>
<UserIdentities>
  <UserIdentity>
    <Name>UserIdentity1</Name>
    <User>testUser</User>
    <PasswordEncrypted>True</PasswordEncrypted>
    <Password>Ewc91LtKh5gu3MyRphF7w==</Password>
    <SupportBasicAuthentication>False</SupportBasicAuthentication>
  </UserIdentity>
  <UserIdentity>
    <Name>UserIdentity2</Name>
    <User>User</User>
    <PasswordEncrypted>False</PasswordEncrypted>
    <Password>SuperSecretPassword</Password>
    <SupportBasicAuthentication>False</SupportBasicAuthentication>
  </UserIdentity>
</UserIdentities>
```

UserIdentities

Main element that holds all user identity definitions.

UserIdentity

Element that holds the definition of a single user identity.

Name

The name of the user identity.

User

The user ID of the user identity.

PasswordEncrypted

Boolean value indicating that the password is encrypted when set to True.

Note: When you export user identities from CES, the XML files generated by CES always contain encrypted passwords.

Password

The password of the user identity (encrypted or not).

SupportBasicAuthentication

Boolean value indicating that CES should allow the use of this user identity in Basic Authentication schemes when set to True.

8.7.4.1.11 Managing Super User Access

As a Coveo administrator, you can grant super user access to a user or a group of users. Use this feature with extreme care for authorized personnel only.
Important:

- For security reasons, all super user access related events are recorded, traceable, and can be audited. CES records who grants super user access to whom as well as all queries performed with a super user access.
- When your Coveo instance connects to a remote index, both Coveo instances must run the same Coveo Enterprise Search version and release number to be able to grant super user access.

You must set an expiration date and can revoke a super user access at any time, but you cannot delete traces that it was granted and traces of its usage.

This topic contains the following sections:

- "Granting super user access" on page 424
- "Revoking super user access" on page 427
- "Monitoring super user access" on page 427

8.7.4.1.11.1 Granting super user access

1. On the Coveo server, access the Administration Tool.

2. Verify that your Coveo license includes the super user access feature:
   
   a. Select Configuration > License.
   
   b. In the License page, validate that Super Users Allowed appears with a check mark.

   When it does not appear and you want to use the super user access feature, contact Coveo Sales to change the license terms.


4. In the panel on the left, select Super User Access.

5. In the panel on the right, click Add.

6. In the Super User Access page:
a. In the **Granted To** section, click **Add**.

b. In the **Add Identity** dialog box, specify the user or group to which you want to grant super user privileges (see "Using the Identity Picker Form" on page 428), and then click **Add**.
The specified user or group appears in the **Granted To** list.

c. Repeat the above steps to add other users or groups to this super user token.

d. In **Description**, enter a short description that describes the scope of the super user token. This text appears in the **Do more** menu when the granted user accesses the .NET search interface.

e. Set the **Start** and **Expiration** dates to specify when the super user access privileges respectively begin and end.

f. Specify the access granted with this super user token:

   i. Select the **Access Everything** check box when you want the users or groups of this super user token to gain access to all indexed contents.

   ii. When the **Access Everything** check box is cleared, in the **Users/Groups** section that appears, click **Add** to select to which user(s) or group(s) permissions the users or groups of this super user token gain access (see "Using the Identity Picker Form" on page 428).

   iii. Repeat the previous step to add other users or groups equivalent permissions.

g. When one or more remote indexes are available, in the **Remote Indexes** section, select the check box for the remote indexes for which you want this super user token to get access to.

   **Note:** In the case where the super user can access remote indexes, the **MismatchingInstance: Instance access is denied.** message may appear. The super user access is granted on the remote Coveo instances only if the remote instance impersonates the user that runs IIS on the Front-End server, typically the \[Server_Name]\$ or the NT Authority\Network Service user (see "Granting Impersonator Privileges" on page 415).

h. Because you cannot edit a super user token once it is created, carefully verify all settings, and then click **Save**.
8.7.4.11.2 Revoking super user access

1. On the Coveo server, access the Administration Tool.
3. In the panel on the left, select Super User Access.
4. In the panel on the right:
   a. Select the super user access that you want to revoke.
   b. Click Revoke.

8.7.4.11.3 Monitoring super user access

1. On the Coveo server, access the Administration Tool.
2. Select Logs > Queries.
3. In the Queries page:
   a. In the panel on the left, select the period over which you want to review the logs as well as the content of the logs, ensuring that the Super User Access check box is selected.
   b. At the top of the panel on the right, click View Log.

   In the logs, the Super User Access column indicates the super user token used, the On behalf column indicates the user that performed the super user queries, and the Full access from index browser column
indicates if the query was performed in the Index Browser.

### 8.7.4.1.12 Using the Identity Picker Form

You must use the identity picker form when you specify a user or group for a security related feature such as assigning an administrator role, granting impersonation, creating a super user, or configuring collaborative rating.

To use the identity picker form

1. In the Coveo Administration Tool, access a page where you must specify a user or group using the identity picker form (see "Assigning Users to Administration Roles" on page 412, "Granting Impersonator Privileges" on page 428.
2. In the identity picker form:

   ![Identity Picker Form](image)

   a. In the **Security Provider** drop-down box, select the security provider to which belongs the desired user or group.
   
   b. In the **Type** drop-down box, select if the desired identity is a **User** or a **Group**.
   
   c. In the **Name** box, enter the name of the user or group that you want to pick.
   
   d. When you selected a security provider (such as a Claims security provider) that has the **Allow Complex Identities** option selected, the **Parameters** section appears to allow you to specify additional identity parameters:
      
      i. Click **Add Parameters**.
      
      ii. In the list that appears, enter the required **Name** and **Value** pair for each required additional parameter.
   
   e. When the form appears in a dialog box, click **Add**.
Example: In a SharePoint on-premises Claims environment, you want to create a super user that emulates a specific group with specific claims to test the content that is accessible to this group.

You select your on-premises SharePoint security provider (that has the Allow Complex Identities option selected), and then can click Add Parameters and enter the claims that you want this super user to have.

8.7.4.2 Administration Tool - Schedules Menu

Coveo Enterprise Search comes with a scheduling mechanism that allows you to automate source content updates and system tasks.

For each of your sources, the best practice is typically to schedule:

- An **Incremental Refresh** at short time intervals to efficiently keep you source closely up-to-date with the repository (see "Scheduling a Source Incremental Refresh" on page 433).

- A **Full Refresh** at longer time intervals to catch possible corner cases that could be missed by the Incremental Refresh (see "Scheduling Source Refresh Actions" on page 435).

The time intervals at which you schedule Incremental Refresh and Full Refresh depend on a number of factors (see "What Should Be the Frequency of Source Refresh Schedules?" on page 441).

8.7.4.2.1 What Is the Purpose of Schedules?

The purpose of schedules is to accomplish recurrent tasks on a regular interval in order to free the Coveo administrator from having to perform these basic operations manually. In other words, schedules maintain the index in its optimal state and let the Coveo administrator focus on more important duties.
Two types of schedules exist:

- Source schedules automatically perform a configurable action on a source (see "Creating or Modifying a Source Schedule" on page 431).
- System schedules perform maintenance tasks such as updating document rating or security cache (see "Modifying System Schedules" on page 439).

### 8.7.4.2.2 Creating or Modifying a Source Schedule

Source schedules allow you to specify the time and interval at which an action can be performed automatically on a source. Coveo Enterprise Search comes with a set of predefined source schedules. You can modify predefined source schedules or create new ones that better suit your needs.

**Example:** You can create custom source schedules tailored for each of your large sources to distribute their refreshing in time to prevent stressing the Coveo and repository server resources.

A best practice is to create and assign one or more custom source schedules for each source with optimized incremental/full refresh intervals (see "What Should Be the Frequency of Source Refresh Schedules?" on page 441). This also allows you to enable/disable a schedule for a source without affecting other sources.

**Note:** A source must have been manually built at least once before a source schedule can rebuild or refresh it.

To create or modify a source schedule

1. On the Coveo server, access the Administration Tool.
2. In the Administration Tool, select **Configuration > Schedules**.
3. In the navigation panel on the left, click **Source Refresh**.
4. In the **Source Schedules** page:
To deactivate/reactivate a source schedule, click [Disable]/[Enable] on the right on the corresponding line.

**Example:** When an indexed repository is put offline, it is recommended to stop indexing the source to prevent unnecessary connection attempts. You can disable the corresponding source schedule.

**Note:** Disabling a schedule from this Administration Tool page, disables the schedule for all sources using the schedule. You can also disable a schedule only for a specific source (see "Disabling a Schedule for a Specific Source" on page 438).

5. When you choose to create or modify a schedule, in the **Schedule** page:
a. In **Schedule Name**, enter a name to identify the schedule.

**Notes:**
- This name is what you will see in the **Refresh Schedule** drop-down list when you configure sources.
- A detailed description is created automatically based on the interval criteria.

**Example:** You create a schedule for the incremental refresh of your corporate Jive site. You could name the schedule: **Jive Corporate site (incremental)**

b. In the **Schedule** section, select the **Enabled** check box, and then select the frequency type (Hourly, Daily, Weekly, Monthly, or Custom interval for interval in minutes) (see “What Should Be the Frequency of Source Refresh Schedules?” on page 441).

c. Use the **Start**, **Start Every**, **Start On** and **Start Only The** parameters to precisely identify when the schedule starts.

**Note:** Avoid setting a schedule to start from 2:00 and 2:59 AM to prevent Daylight Saving Time (DST) issues. [more]

d. When you are modifying an existing schedule, in the **Used By** section:
   i. Verify if the source schedule is already assigned to one or more sources.
   ii. When it is the case, verify if the modifications are appropriate for all assigned sources.
   iii. When not appropriate, rather consider creating a new source schedule, or change source schedule assignments.

e. Click **Save/Apply Changes**.

**What's Next?**

Assign the refresh schedule to one or more sources (see "Scheduling Source Refresh Actions" on page 435).

### 8.7.4.2.3 Scheduling a Source Incremental Refresh

Incremental refresh is a feature that is available for most connectors. It allows your to efficiently keep a source up-to-date by re-indexing at short time intervals only the documents reported by the repository to be new, modified, or deleted since the last incremental refresh.

Once a source is created and indexed at least once, you must manually set an incremental refresh schedule for your source.
Notes:

- You do not have to worry about overlapping Full Refresh and Incremental Refresh schedules:
  - A scheduled Full Refresh/Rebuild automatically stops a running Incremental Refresh before starting.
  - A scheduled Incremental Refresh is ignored while a Full Refresh/Rebuild is running.
- CES 7.0.6942 – (August 2014) You cannot add or delete a schedule while a source is being indexed.

To configure an incremental refresh schedule for a source

1. On the Coveo server, access the Administration Tool.
2. Access the Sources and Collections page (Index > Sources and Collections).
3. In the Collections section, click the collection that contains the source for which you want to configure the incremental refresh schedule.
4. In the Sources section, click the appropriate source.
5. In the navigation panel on the left, select Schedules.
6. In the Schedules page:
   a. Click Add to create a new schedule or click an existing one to modify it.
   b. In the Action drop-down list, select Start.
   c. In the Type section, select Incremental Refresh.

   **Note:** When the Incremental Refresh option is not present, the source type does not support incremental refresh.
d. In the **Schedule** drop-down list, select an appropriate time interval for the incremental refresh (see "What Should Be the Frequency of Source Refresh Schedules?" on page 441).

**Note:** Click **Manage Schedules** to modify existing refresh schedules or create new ones with time intervals that are more appropriate to your environment (see "Creating or Modifying a Source Schedule" on page 431).

e. Click **Apply Changes**.

To disable an incremental refresh schedule for a source

**Example:** When a repository indexed by a source is offline, it is recommended to disable incremental refresh to prevent unnecessary unsuccessful connection attempts to the repository.

1. On the Coveo server, access the Administration Tool.
2. Access the **Sources and Collections** page (**Index > Sources and Collections**).
3. In the **Collections** section, click the collection that contains the source for which you want to disable the incremental refresh schedule.
4. In the **Sources** section, click the appropriate source.
5. In the navigation panel on the left, select **Schedules**.
6. In the **Schedules** page, at the end of the line for the schedule that you want to disable, click **[Disable]**.

<table>
<thead>
<tr>
<th>Schedules</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image" alt="Add" /> <img src="image" alt="Delete" /></td>
</tr>
</tbody>
</table>

**8.7.4.2.4 Scheduling Source Refresh Actions**

You can use predefined or custom source schedules to automate actions on a source at specific times and intervals. By default, the **Every day** schedule is applied to newly created sources to start a source full refresh everyday at 12 A.M.

A best practice is to create and assign one or more tailored custom schedules for each source with optimized incremental/full refresh intervals (see "What Should Be the Frequency of Source Refresh Schedules?" on page 441). This also allows you to distribute the refreshing of your various sources over time and to enable/disable a schedule for a source without affecting other sources.

When incremental refresh is available for a source type, you will typically assign two schedules to a source:
Incremental Refresh scheduled at short intervals based on content change rate (see "Scheduling a Source Incremental Refresh" on page 433).

Full Refresh scheduled at longer intervals such as weekly.

Notes:

- You do not have to worry about overlapping Full Refresh and Incremental Refresh schedules:
  - A scheduled Full Refresh/Rebuild automatically stops a running Incremental Refresh before starting.
  - A scheduled Incremental Refresh is ignored while a Full Refresh/Rebuild is running.

- CES 7.0.6942–(August 2014) You cannot add or delete a schedule while a source is being indexed.

To schedule a source refresh action

1. On the Coveo server, access the Administration Tool.

2. Access the Sources and Collections page (Index > Sources and Collections).

3. In the Collections section, select the collection that contains the source to which you want to assign a refresh schedule.

4. In the Sources section, select the source to which you want to assign a schedule.

5. In the navigation panel on the left, select Schedules

6. In the Schedules page:

   a. Click an existing schedule to modify its configuration.

   OR

   Click Add to assign a new schedule to this source.

   b. In the page that appears:
In the Action drop-down list, select the desired action:

- **Start** to start either an **Incremental Refresh**, a **Full Refresh** or a **Rebuild**.

- **Pause**, **Resume**, or **Stop** to act on an ongoing source refresh (**Incremental Refresh**, **Full Refresh** or **Rebuild**).

**Example:** A full refresh of your CRM source starts every weekday at midnight. On Wednesdays, between 1:00 and 4:00 AM, your CRM is scheduled for maintenance, so you want to ensure that the source is not indexed during this period by scheduling a refresh **Pause** and a **Resume** at corresponding time.

**Notes:**

- If you pause, and then resume an ongoing source refresh, once the refresh is completed, you should perform a full refresh to ensure the integrity of the source.

- When no **Incremental Refresh**, **Full Refresh**, or **Rebuild** is ongoing, a **Resume** does nothing.

In the **Type** section, select the type of refresh to start:

- **Incremental Refresh** to index only modified documents since the last incremental refresh (see "Incremental Refresh" on page 441).
Note: When the **Incremental Refresh** option is not present, the source type does not support incremental refresh.

- **Full Refresh** to index only modified documents (see "Full Refresh" on page 442).
- **Rebuild** to completely re-index all documents of a source (see "Rebuild" on page 442).

**Important:** It is not recommended to schedule to regularly **Rebuild** a source, particularly for large sources, because each rebuild temporarily increases the size of the index and the load on the index compaction process (see "About the Index Self-Optimization Process" on page 270).

7. **Repeat the previous step when you want to assign another schedule to the source.**

**Note:** You can enable/disable a source refresh schedule for example when repositories are offline to prevent unnecessary connection attempts (see "Creating or Modifying a Source Schedule" on page 431).

### 8.7.4.2.5 Disabling a Schedule for a Specific Source

Once a schedule is configured for a source (see "Scheduling Source Refresh Actions" on page 435 or "Scheduling a Source Incremental Refresh" on page 433), you can toggle the state of a schedule only for this source without loosing the schedule configuration.

**Example:** In your Coveo staging environment, you can configure and test schedules for your sources, and then disable the schedules to prevent unnecessary access to the repositories.

#### To disable/re-enable a schedule for a specific source

1. On the Coveo server, access the Administration Tool.
2. In the Administration Tool, select **Index > Sources and Collections**.
3. In the **Sources and Collections** page:
   a. In the **Collections** section, select the collection containing the source for which you want to disable/enable the schedule.
   b. In the **Sources** section, select the source.
4. In the **Source** page:
   a. In the navigation panel on the left, select **Schedules**.
   b. In the **Schedules** list, at the end of the line of the schedule for which you want to toggle the state, click **[Disable]/[Enable]**, respectively to deactivate and reactivate the schedule only for this source.
The icon identifies an enabled schedule, while the icon identifies a disabled schedule.

8.7.4.2.6 Modifying System Schedules

System schedules perform maintenance tasks on a regular interval to keep the index in an optimal state. Each task has its own schedule. You should plan your CES system schedules and consider synchronizing some of them with other processes (see "What Should Be the Frequency of System Schedules?" on page 442).

To modify a system schedule

1. On the Coveo server, access the Administration Tool.
2. Select Configuration > Schedules.
3. In the navigation panel on the left, click System.
4. In the System page, under System Schedules, you can configure the schedule for the following actions:
   - Set the index to the read-only mode
   - Set the off-peak period
   - Suspend indexing
   - Update document rating
   - Update the security cache
To activate/deactivate a system schedule, click [Enable]/[Disable] on the right on the corresponding line.

OR

To modify a system schedule:

a. Click the system schedule that you want to modify.

b. In the corresponding Schedule page, system schedules have different sets of parameters to allow you to set the moment and interval at which actions are taken:

   i. Next to Schedule, select the Enabled check box.

   ii. Set the available parameters to configure the schedule as you wish.
iii. Click **Apply Changes**.

### 8.7.4.2.7 What Should Be the Frequency of Source Refresh Schedules?

The purpose of source refresh schedules is to ensure that the index content is kept up-to-date.

The source refresh time interval that you select determines the freshness of the index for this source, it should be following the rate of change of documents in the source, but should be optimized to avoid useless connections between the CES and repository servers that can contribute to load both servers.

**Note:** You can create new or modify existing source refresh schedules.

You can schedule the following types of refresh:

- "Incremental Refresh" on page 441
- "Full Refresh" on page 442
- "Rebuild" on page 442

**Note:** For repositories with API call restrictions (such as cloud repositories), consider setting your source refresh frequencies to optimally consume your available API calls.

#### 8.7.4.2.7.1 Incremental Refresh

Many Coveo connectors come with the incremental refresh feature that allows to constantly maintain the index up-to-date with new, modified, or deleted source documents. When available for a source type, it is strongly recommended that you schedule an incremental refresh for your sources (see "Scheduling a Source Incremental Refresh" on page 433).

Choose an incremental refresh time interval that is of the order of magnitude of the rate at which documents change in the source.

**Examples:**

- For a team collaboration Confluence source with a large number of active users where every hour some wiki pages change and several comments are added, select **Every 30 minutes** to make these changes searchable not too long after they have been saved.

- For a relatively static Intranet source where only a few documents are added, modified, or deleted on average everyday, selecting **Every weekday** may be appropriate.

- For a permanently static legacy repository where no document will ever change, do not configure an incremental refresh.

**Note:** Incremental refresh may be not available for a connector type either because the connector rather offers live monitoring (see "About Incremental Refresh and Live Monitoring" on page 308) or because the repository or the connector does not support it.
8.7.4.2.7.2 Full Refresh

When incremental refresh or live monitoring is configured, it is generally recommended to set a source full refresh to a weekly time interval such as Every Sunday.

A weekly full refresh schedule is a safety net to ensure the index stays up-to-date with your source. A weekly full refresh will pick up corner case changes that could be missed by incremental refresh or live monitoring. Also, the incremental refresh of some connectors are known to have limitations (often due to repository API limitations) such as not being able to track deleted documents or permission changes.

When neither incremental refresh or live monitoring is available for a source, choose a full refresh time interval in relation with the rate of change of source content to ensure an acceptable index freshness without overloading the CES and repository servers.

**Examples:**

A repository source without incremental refresh contains a relatively small number of documents and several documents are added, modified, or deleted every day, selecting a refresh schedule of Every 6 hours would be appropriate.

For a permanently static legacy repository where no document will ever change, select (none) as no regular refresh is appropriate.

8.7.4.2.7.3 Rebuild

It is generally not recommended to create refresh schedules of Rebuild type, particularly for large sources, because each rebuild temporarily increases the size of the index and increases the load on the index compaction process (see "About the Index Self-Optimization Process" on page 270).

Rebuilding a source should be done manually when it is needed, for example following a source configuration change (see "Applying an Action to a Collection or a Source" on page 283).

8.7.4.2.8 What Should Be the Frequency of System Schedules?

The purpose of system schedules is to perform maintenance tasks at regular intervals to keep the index in an optimal state. You can change the system schedules (see "Modifying System Schedules" on page 439).

Refer to the following guidelines to set the frequency of system schedules, sometimes in relation with the schedule of third party systems.

**Read-Only Mode**

- Backups

**Important:** It is recommended to use the CES backup feature to efficiently create index backups. The feature takes care of switching the index to the read-only mode before the backups and back to the read-write mode once it is completed (see "About the Index Backup Feature" on page 205). In this case, you do not need to set the Read-Only Mode schedule.

If you must use the manual backup method (see "Manually Backing Up and Restoring the Index" on page 215) or a third party backup tool, CES must be in read-only mode while you back up your index. Coordinate
the Read-Only Mode schedule to set its period to switch the index mode before your scheduled backup starts and switch it back after the backup is completed.

- Virus scans

CES must also be in read-only mode while you perform a virus scan on your index files. Be aware that it is recommended to exclude the CES index files from the virus scan (see "CES and Anti-Virus Software" on page 232). If you have to scan index files, coordinate the Read-Only Mode schedule to set its period to switch the index mode before your scheduled virus scan starts and switch it back after the scan is completed.

**Note:** You can also switch between index modes manually, which may be useful when the time required to complete a backup or a virus scan is difficult to predict (see "Toggling the Index Between the Read-Write and Read-Only Modes" on page 263).

**Off-Peak Period**

Enable this schedule for the periods over which your Coveo servers receive a lower number of queries.

During this period, CES automatically runs or intensifies background processes such as:

- Index self-optimization process (see "About the Index Self-Optimization Process" on page 270)
- Rebuild the Word Correction Lexicon
- Calculation of the stem classes for queried words

**Suspend Indexing**

As a temporary measure, consider enabling and configuring a **Suspend Indexing** schedule if CES is slowed down when many users query the index. Indexing can be suspended to devote maximum CPU resources to querying. You can identify the peak querying hours, during which to suspend indexing (see "What Information Is Displayed in the Query History?" on page 386). However, if querying peaks occur at irregular intervals, it is possible to disable and re-enable indexing manually (see "Disabling or Enabling Indexing" on page 269).

**Update Document Rating**

It is recommended to update document ratings at least once a week. However, if collaborative rating has a high ranking weight, it is recommended to update ratings every one or two days to preserve ranking precision.

**Update Security Cache**

It is recommended to update the CES security cache daily to synchronize the cache with all security entities (users and groups) changes from all indexed repositories (see "What Is a Security Cache?" on page 264).

Updating the cache sends requests to all repositories to get all users and groups. Returning this information may be resource intensive for servers of some repository types when there is a large number of users and groups. This is why by default, the security cache update is scheduled only once a day during a typical off-peak period. Consider changing the time at which the **Update Security Cache** schedule starts daily to distribute scheduled processes running on your Coveo and repository servers.

When permissions modifications in repositories must be taken into account rapidly, such as when a new user must access restricted documents before the next scheduled update, you can also update the security cache
manually only for selected security entities (see Using the Security Browser) or for the all security entities (see "Refreshing Security Caches" on page 266).

8.7.4.2.9 Schedules and Daylight Saving Time

A schedule programmed to start during the Daylight Saving Time (DST) change interval will not operate normally.

At the start of the DST period, when clocks are adjusted forward from 2:00 to 3:00 AM, schedules programmed to start between 2:00 and 2:59 AM inclusively will not start. Furthermore, weekly and monthly schedules programmed to start between 2:00 and 2:59 AM inclusively on any day during the following week will also not start.

**Example:** On Sunday, March 9, 2014, the clock of a Coveo server running in the USA is adjusted forward at 2:00 AM. A CES weekly schedule programmed to start on Friday, March 14 at 2:15 AM does not start because it occurs within one week following the DST forward adjustment.

At the end of the DST period, when clocks are adjusted backward from 3:00 to 2:00 AM, schedules programmed to start between 2:00 and 2:59 AM will start twice.

To prevent these issues, it is therefore recommended to avoid programming a schedule to start during the DST clock adjustment time interval (typically between 2:00 and 2:59 AM).

8.7.4.3 Administration Tool - Connectors Menu

In the **Connectors** menu, for each available connector, you can configure parameter values that apply by default to all sources using this connector.

8.7.4.3.1 Adding a Connector

A number of connectors are available out-of-the-box with the Coveo Platform. You can also add other custom or prototype connectors to your CES configuration to be able to index other repositories and systems.

**Example:** Your in-house programmers, Coveo Professional Services, or a third party, developed a connector for your custom CMS system so that you can bring its content into your Coveo unified index.

**Note:** You can also contact the Coveo Professional Services to get assistance to develop your own connectors for example for in-house custom repositories/systems using the Open Connector API.

To add an additional connector

1. Get the connector files, ensuring that they are compiled for your version and release of CES. Ask for the name of the class implementing the connector.
   - For a documented prototype connector, contact Coveo Support.
   - For a custom connector, contact whoever developed the connector (Coveo Professional Services, in-house, or third-party developer).

2. Using an administrator account, connect to the Coveo Master server.

3. Copy the connector files to the [CES Path]\Bin folder.
Example: On a 64-bit server, copy 64-bit versions of the connector files to the C:\Program Files\Coveo Enterprise Search 7\Bin folder. If you have a 32-bit version of the connector files, copy them to the C:\Program Files\Coveo Enterprise Search 7\Bin\Win32 folder.

4. On the Coveo server, access the Administration Tool.

5. Select Configuration > Connectors.

6. In the Connectors page, the currently available connectors are listed. Click Add.

7. In the navigation panel on the left, click Additional Connector.

8. In the Additional Connectors page, click Add.

9. In the Connectors page, enter appropriate values for the following parameters:

   ![Connectors page](image)

   **Name**
   
   A name of your choice to identify the additional connector.

   **Description**
   
   A description of the type of repository indexed by the connector.

   **Assembly Path**
   
   The full path of the additional connector assembly file.

   Example: C:\Program Files\Coveo Enterprise Search 7\Bin\Crawlers\Coveo.CES.CustomCrawlers.Custom1.dll
Note: If the path is incomplete, CES searches for the assembly file in its [CES_Path]\bin directory (by default, C:\Program Files\Coveo Enterprise Search 7\Bin).

**Type Name**

The name of the class implementing the connector.

**Note:** The parameter is optional when only one class is inheriting from the `CustomCrawlers` class. When this is the case, you can leave the box empty.

**Example:** Coveo.CES.CustomCrawlers.ODBC.ODBCCrawler

**Parameters**

Allows you to define explicit parameters. Click **Add Parameter** to display the Modify the parameters of the additional connector page (see "Adding an Explicit Connector Parameter" on page 450).

You must add the following parameters to get the **Security** section in the **Add Source** page for sources of this type and allow you to specify the security provider and user identity that the source will use.

<table>
<thead>
<tr>
<th>Type</th>
<th>Name</th>
<th>Label</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security Provider</td>
<td>SecurityProvider</td>
<td>Security Provider</td>
</tr>
<tr>
<td>User Identity</td>
<td>UserIdentity</td>
<td>Authentication</td>
</tr>
</tbody>
</table>

**Options**

For 64-bit servers, select the **Run in 64 bits** check box to instantiate the connector in a 64-bit process.

**Number of concurrent sources**

Specify the maximum number of sources using this connector that can operate concurrently.

10. Click **Save**.

### 8.7.4.3.2 Customizing a Connector

The main reason to customize a connector is often to add explicit parameters. However, you may also need to modify the connector description, its assembly path when you move it from the original location, or the type name when the name of the class implementing the connector is modified.

To customize a connector

1. On the Coveo server, access the Administration Tool.
2. Select **Configuration > Connectors**.
3. In the **Connectors** page, click the connector that you want to modify.
4. In the page that appears, edit the parameters that you want to modify. The available parameters vary...
depending on the connector type.

**Example:** The following capture shows the Confluence connector parameters.

![Confluence connector parameters](image)

Typical connector parameters are:

**Description**

A description of the type of repository indexed by the connector.

**Assembly Path**

The full path of the additional connector assembly file.

**Example:** `D:\CES7\Index\Crawlers\Coveo.CES.CustomCrawlers.Custom1.dll`

**Note:** If the path is incomplete, CES searches for the assembly file in its `[CES_Path]\bin` directory (by default, `C:\Program Files\Coveo Enterprise Search 7\Bin`).

**Type Name**

The name of the class implementing the connector.

**Example:** `Coveo.CES.CustomCrawlers.ODBC.ODBCCrawler`

**Parameters**

Allows to define explicit parameters. Click **Add Parameter** to display the **Modify the parameters of the**
connector page (see "Adding an Explicit Connector Parameter" on page 450).

Options

Select the Allow Custom parameters check box to be able to create dynamic parameters (see "Adding a Dynamic Parameter to a Connector Source" on page 453).

For 64-bit servers, select the Run in 64 bits check box to instantiate the connector in a 64-bit process.

Number of concurrent sources

Specify the maximum number of sources using this connector that can operate concurrently.

5. Click Apply Changes.

8.7.4.3.3 What Is the Difference between Explicit and Dynamic Parameters?

Explicit parameters apply to all sources indexed using the connector—for this reason, they are created directly in the Modify Additional Connector page. They are used to input information common to all repositories (ex.: the username and password required to access databases). You can see and modify explicit parameters in the Connectors page for a specific connector (see "Adding an Explicit Connector Parameter" on page 450).
Example: The Connectors page for the Desktop connector.

Dynamic parameters apply to a single source and are created in the Add Source page. They are used to adapt indexing to a specific repository (see "Adding a Dynamic Parameter to a Connector Source" on page 453).
Example: The Add Source page for a Desktop connector source.

Connector parameters applying to all sources indexed using this connector are called explicit parameters.
When you create or configure a source, the Coveo Enterprise Search (CES) 7.0 Administration Tool presents parameters with which you can configure the connector for most setups. For many connectors, more advanced and more rarely used parameters also exist but are hidden by default. CES then uses the default value associated with each of these hidden parameters.

You can however choose to make one or more of these parameters appear in the Add Source and Source: ... General pages of the Administration Tool so that you can change their default value.

To add an explicit connector parameter

1. On the Coveo server, access the Administration Tool.
2. Select Configuration > Connectors.
3. In the list on the Connectors page, select the connector for which you want to show advanced hidden parameters.
4. In the Parameters section of the selected connector page, click Add Parameter for each hidden parameter that you want to modify.

   **Note:** The Add Parameter button is present only when hidden parameters are available for the selected connector.

5. In the Modify the parameters of the connector page:

   ![Modify the parameters of the connector](image)

   a. In the **Type** list, select the parameter type as specified in the parameter description.
   b. In the **Name** box, type the parameter name exactly as it appears in the parameter description. Parameter
names are case sensitive.

c. In the **Default Value** box, enter the default value specified in the parameter description.

   **Important:** Do not set the value that you want to use for a specific source. The value that you enter here will be used for all sources defined using this connector so it must be set to the recommended default value. You will be able to change the value for each source later, in the **Add Source** and **Source:** ... **General** pages of the Administration Tool.

d. In the **Label** box, enter the label that you want to see for this parameter.

   **Example:** To easily link the label to the hidden parameter, you can simply use the parameter name, and if applicable, insert spaces between concatenated words. For the **BatchSize** hidden parameter, enter *Batch Size* for the label.

   **Note:** To create multilingual labels and quick help messages, use the following syntax:

   <@ln>text</@>, where *ln* is replaced by the language initials—the languages of the Administration Tool are English (en) and French (fr).

   **Example:** <@fr>Chemin d'accès du fichier de configuration</@><@en>Configuration File Path</@> is a label which is displayed differently in the French and English versions of the Administration Tool.

   **Tip:** The language of the Administration Tool can be modified by pressing the following key combination: Ctrl+Alt+Page Up.

e. Optionally, in **Quick Help**, enter the help text that you want to see for this parameter when clicking the question mark button that will appear beside the parameter value.

   **Tip:** Copy and paste key elements of the parameter description.

f. When **Predefined values** is selected in the **Type** parameter, in the **Value** box that appears, enter the parameter values that you want to see available in the drop-down parameter that will appear in the Administration Tool interface. Enter one value per line. The entered values must exactly match the values listed in the hidden parameter description.

g. Select the **Optional parameter** check box when you want to identify this parameter as an optional parameter. When cleared, CES does not allow you to save changes when the parameter is empty. This parameter does not appear for **Boolean** and **Predefined values** parameter types.

h. Select the **Sensitive information** check box for password or other sensitive parameter so that, in the Administration Tool pages where the parameter appears, the typed characters appear as dots to mask them. This parameter appears only for the **String** type.

   **Example:** When you select the **Sensitive information** check box for a parameter, the characters typed appear as follows in the text box:

   ![Sensitive information example](image)

i. Select the **Validate as an email address** check box when you want CES to validate that the text string that
a user enters in this parameter respects the format of a valid email address. This parameter appears only for the **String** type.

j. In the **Maximum length** box, enter the maximum number of characters for the string. This parameter appears only for the **String** type. When you enter 0, the length of the string is not limited.

k. Click **Save**.

6. Back in the **Connector** page, click **Apply Changes**.

The hidden parameter now appears in the **Add Source** and **Source: ... General** pages of the Administration Tool for the selected source. You can change the parameter value from these pages. Refer to the documentation for each connector for details.

**Note:** When you want to modify a hidden source parameter, you must first delete it, and then redefine it with the modified values.

### 8.7.4.3.5 Adding a Dynamic Parameter to a Connector Source

Dynamic parameters apply to a single source and are created in the **Add Source** page. They are used to adapt indexing to a specific repository.

Before adding dynamic parameters, you must first ensure that a connector is configured to allow dynamic parameters to be added sources of this type.

**To allow the creation of dynamic parameters for a connector**

1. On the Coveo server, access the Administration Tool.

2. Select **Configuration > Connectors**.

3. In the **Connectors** page, click the connector for which you want to enable the addition of dynamic parameters to sources using this connector.

4. In the page that appears, in the **Options** section, select the **Allow custom parameters** check box.

5. Click **Apply Changes**.

**To create a dynamic parameter for a connector source**

1. On the Coveo server, access the Administration Tool.

2. Select **Index > Sources and Collections**.

3. In the **Sources and Collections** page:
   a. Under **Collections**, select the collection containing the source to which you want to add a dynamic parameter.
   b. Under **Sources**, select the source.

4. In the page for the source:
a. In the navigation panel on the left, select General.

b. In the panel on the right, in the Parameters section, click Add Parameter.

Two boxes appear.

<table>
<thead>
<tr>
<th>Name</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Delete

Add Parameter

Coveo

Coveo Platform 7.0 | Administrator Guide

Example: When the name entered is port, the connector searches for a port field to submit the value.

c. In the Name box, enter the name of the field in which the parameter value is submitted.

d. In the Value box, enter the value submitted by the connector.

e. Click Apply Changes.

8.7.4.3.6 Selecting a 32-bit or 64-bit Process for a Connector

On a 64-bit Coveo server, many connectors can run either in a 32-bit or 64-bit process. Setting a connector to run in 64-bit allows to take advantage of the 64-bit performance. However, in some cases, connectors need to run in a 32-bit process.

Example: When indexing PST mail archive files, the File connector uses a third-party library that does not support 64-bit processes and must therefore run in a 32-bit process.

Important: Selecting a 32-bit or 64-bit process for a connector affects all sources for this connector. Changing the state of the Run in 64 bits check box requires a refresh of all the sources of this connector.

To select a 32-bit or 64-bit process for a connector

1. On a 64-bit Coveo server, access the Administration Tool.

2. Select Configure > Connectors.

3. In the Connectors page, select the connector that you want to modify.

4. In the page for the connector:

   a. In the Option section, select or clear the Run in 64 bits check box when you want the connector to run respectively in a 64-bit or 32-bit process.

   b. Click Apply Changes.

   Note: You may need to restart the CES service to make changes effective (see “Starting the CES Service” on page 248).

5. Refresh all the sources for this connector.
8.7.4.4 Administration Tool - Converters Menu

Converters are responsible for extracting content and properties from documents in order to add them to the index. Once a document is crawled by one of the Coveo connector, a converter must be used before the document can be added to the index.

CES comes with several native converters that extract the content and properties of the most popular document types, including MS Office files, PDF files, Web pages, etc.

While the default conversion process normally suffices to handle most CES deployments, CES offers a rich development API to enhance and tweak the way documents are converted and indexed (see "What Are the Conversion Phases?" on page 455).

The Open Converter API offers the following advantages (see Converter API Home):

- Ability to convert and index documents from any format using the custom converters and the "What Are IFilters?" on page 482 technologies.
- Tweak the conversion process using conversion scripts in multiple hook points.

Remote Converters

It is possible to add remote converters on different servers to distribute the converting process between CPUs and, therefore, speed up indexing (see "Installing CES Remote Converter Components" on page 62 and "Configuring a Remote Converter" on page 458).

8.7.4.4.1 What Are the Conversion Phases?

The following lists the different phases of the conversion process:

1. **Crawling**: In this phase, the document will be fetched using a connector (file, Exchange, SharePoint, etc.). Some metadata will already be made available by the connector, including the URI, modification date and much more.

2. **Global Preconversion script (optional phase)**: If a global preconversion script has been set, this script will be executed in this phase. Common script tasks: Read document content, read and modify metadata, update document permissions, etc.

3. **Source Preconversion script (optional phase)**: If a preconversion script has been set on the document source, this script will be executed in this phase. Common script tasks: Read document content, read and modify metadata, update document permission, etc.

4. **Open Converter (optional phase)**: If the Document Type has been set to convert the document using an open converter, this script will be executed in this phase. Common script tasks: Convert the document from an unsupported format to a CES native format, read and modify metadata, update document permission, etc.

5. **Native Converter**: In this phase, the document content and properties will be extracted using one of the native CES converters.

6. **Document Text Analysis**: Many proprietary analysis technologies will be used to generate a document summary and key concepts, perform a language and title detection, and much more.

7. **Source Postconversion script (optional phase)**: If a postconversion script has been set on the document
source, this script will be executed in this phase. Common script tasks: Update the document extracted text and HTML, read and modify metadata, reject documents, etc.

8. **Global Postconversion script (optional phase)**: If a global postconversion script has been set, this script will be executed in this phase. Common script tasks: Update the document extracted text and HTML, read and modify metadata, update document permission, etc.

9. **Index the document.** This phase will put the document extracted content and properties into the Coveo unified index to make it available for user queries.
Conversion phases

1. Connector

2. Is a global preconversion script available?
   - Yes → Global preconversion script
   - No → 3

3. Is a source preconversion script available?
   - Yes → Source preconversion script
   - No → 4

4. Does the document conversion need an open converter?
   - Yes → Open converter
   - No → 5

5. Native converter

6. Text analysis

7. Is a source postconversion script available?
   - Yes → Source postconversion script
   - No → 8

8. Is a global postconversion script available?
   - Yes → Global postconversion script
   - No → 9

9. Index
8.7.4.4.2 Configuring a Remote Converter

When you have a large number of documents to convert that require either too much resources from the Master server or too much time to complete, you can use other servers to convert documents.

By default, the CES remote converter components are installed on Mirror servers. You can also install the remote converter components on one or more dedicated servers (see "Installing CES Remote Converter Components" on page 62).

Once you deployed the CES remote converter components on one or more servers, you must configure the Coveo Master server to use them.

To configure a remote converter

1. Using an administrator account, connect to the Coveo Master server.
2. Access the Administration Tool (see "Opening the Administration Tool" on page 256).
3. In the Administration Tool, select Configuration > Converters.
4. In the Converter Managers page, click Add.
5. In the Add Converter Manager page:

   a. In the Name box, enter a name of your choice to identify the remote converter.

      **Example:** Simply use the hostname of the Remote Converter or Mirror server that you want to use.

   b. In the Location box, enter the hostname or IP address of the server on which the CES remote converter
components are installed.

c. In the Threads box, enter the number of simultaneous downloads handled by the converter. Two threads is the maximum recommended for a single CPU, more threads may slow down CES.

d. In the OCR Threads box, enter the number of simultaneous threads to be used by the optical character recognition (OCR) Module, respecting the limit of your OCR Module license (see OCR Module).

e. In the Thread Priority drop-down list, select the priority of the converting process compared to other processes that are running on the Remote Converter server.

Example: When you use the remote converter components from a Mirror server, consider selecting Below Normal to minimize the impact on the primary process of the server.

f. Configure the parameters of the Enhanced Quick View section (see "Installing the Enhanced Quick View Components" on page 472).

g. Click Save.

When an error message appears at the top of the page, refer to the following list to troubleshoot the problem, make appropriate changes, and then click Apply Changes.

Cannot create remote converter on hostname. The RPC server is unavailable.

- Ensure that the firewalls on both machines are not blocking the DCOM communications between the servers.

Cannot create remote converter on hostname. Access is denied.

- Ensure that the CES service logon account of the Master server is a specific account that has administrator rights on the Remote Converter server as well (see "About the CES Service Logon Account" on page 225).

8.7.4.4.3 Adding an Open Converter

Open converters, written in .NET, VBScript, or JScript, are used to index document types not natively supported by Coveo Enterprise Search.

To add an open converter

1. On the Coveo server, access the Administration Tool.
2. Select Configuration > Converters.
3. In the Converter Managers page, in the navigation panel on the left, click Open Converters.
4. In the Open Converters page, click Add.
5. In the Add an Open Converter page:
a. In the **Name** box, enter a name to identify the open converter.

b. In the **Script File** box, click **...** to browse or enter the complete path of the open converter file.

c. In the **Script Language** drop-down list, select the language in which the open converter is written.

d. When the **Script Language** is set to **.NET**, in the **Type Name** box, enter the name of the class in the **.NET** assembly that implements the converter.

e. If the open converter requires one or more parameters, for each parameter, in the **Parameters** section, click **Add Parameter**, and then enter the name and value of the parameter.

f. Click **Apply Changes**.

### 8.7.4.4.4 Adding a Preconversion Script

Preconversion scripts, written in **.NET**, **VBScript**, or **JScript**, are used to manipulate document properties before the conversion.

**Example:** With a preconversion script, you can add a specific document metadata.

To add a preconversion script

1. On the Coveo server, access the Administration Tool.

2. Select **Configuration > Converters**.

3. In the **Converter Managers** page, in the navigation panel on the left, click **Conversion Scripts**.

4. In the **Conversion Scripts** page is displayed, above the **Preconversion Scripts** section, click **Add**.

5. In the **Add a Preconversion Script** page:
a. In the **Name** box, enter a name to identify the conversion script.

b. In the **Script File** box, click ![browse](#) to browse or enter the complete path of the conversion script file.

   **Tip:** It is a good practice to store conversion script files under the [Index_Path]\Config\ folder (such as in C:\CES7\Config\Scripts\) so that your script files are backed up with the other configuration files (see "Backing Up and Restoring the CES Configuration Files" on page 216).

   **Note:** For .NET scripts, you can select the DLL or the .cs file, in which case, CES automates the compilation of the on-demand. Furthermore, when you update the source file, CES automatically uses the updated file so you do not need to explicitly reload the .NET script file from the Administration Tool.

c. In the **Script Language** drop-down list, select the language in which the conversion script is written.

   **Note:** When selecting **JScript**, ensure that your code uses only statements supported by JScript, the Microsoft JavaScript dialect (see **JScript Reference**).

   **Example:** JScript does not support the JavaScript **forEach** statement. You must rather use more basic loop statements (see **Loops in JScript**).

d. When the **Script Language** is set to **.NET**, in the **Type Name** box, enter the name of the class in the .NET assembly that implements the conversion script (see "About .NET Conversion Scripts" on page 463).

e. If the conversion script requires one or more parameters, for each parameter, in the **Parameters** section, click **Add Parameter**, and then enter the name and value of the parameter.

   f. Click **Save**.
Once you apply the script to a source, on the script page, the source name will appear next to **Used By**.

**What's Next?**

Apply the conversion script globally to all collections and sources of the index or to a specific source (see "Applying a Global Conversion Script" on page 464 and "Applying a Source Conversion Script" on page 465).

### 8.7.4.4.5 Adding a Postconversion Script

Postconversion scripts, written in .NET, VBScript, or JScript, are used to manipulate document properties after the conversion.

**Example:** With a postconversion script, you can update the document concepts and summary sentences.

To add a postconversion script

1. On the Coveo server, access the Administration Tool.
2. Select **Configuration > Converters**.
3. In the **Converter Managers** page, in the navigation panel on the left, click **Conversion Scripts**.
4. In the **Conversion Scripts** page is displayed, above the **Postconversion Scripts** section, click **Add**.
5. In the **Add a Postconversion Script** page:
   - In the **Name** box, enter a name to identify the conversion script.
   - In the **Script File** box, click ![Browse](image) to browse or enter the complete path of the conversion script file.
Tip: It is a good practice to store conversion script files under the [Index_Path]\Config\ folder (such as in C:\CES7\Config\Scripts\) so that your script files are backed up with the other configuration files (see "Backing Up and Restoring the CES Configuration Files" on page 216).

Note: For .NET scripts, you can select the DLL or the .cs file, in which case, CES automatically compiles the file on-demand. Furthermore, when you update the source file, CES automatically uses the updated file so you do not need to explicitly reload the .NET script file from the Administration Tool.

c. In the Script Language drop-down list, select the language in which the conversion script is written.

Note: When selecting JScript, ensure that your code uses only statements supported by JScript, the Microsoft JavaScript dialect (see JScript Reference).

Example: JScript does not support the JavaScript forEach statement. You must rather use more basic loop statements (see Loops in JScript).

d. When the Script Language is set to .NET, in the Type Name box, enter the name of the class in the .NET assembly that implements the conversion script (see "About .NET Conversion Scripts" on page 463).

e. If the conversion script requires one or more parameters, for each parameter, in the Parameters section, click Add Parameter, and then enter the name and value of the parameter.

f. Click Save.

CES 7.0.9434+ (September 2018) Once you apply the script to a source, on the script page, the source name will appear next to Used By.

What's Next?

Apply the conversion script globally to all collections and sources of the index or to a specific source (see "Applying a Global Conversion Script" on page 464 and "Applying a Source Conversion Script" on page 465).

8.7.4.4.6 About .NET Conversion Scripts

Previously, preconversion and post conversion scripts could only be written using VBS or JScript languages. These languages offer no debugging support and limited functionalities.

With CES 7, you can now also create C# preconversion or postconversion scripts. You can select the DLL or the .cs file, in which case, CES automatically compiles the file on-demand. Furthermore, when you update the source file, CES automatically uses the updated file so you do not need to explicitly reload the .NET script file from the Administration Tool (see "Adding a Preconversion Script" on page 460 and "Adding a Postconversion Script" on page 462).

Note: When using .NET source code rather than the compiled DLL, you must explicitly declare the optional parameters.

You can debug your .NET scripts with Visual Studio. Simply attach to the CESConverter7.exe process and put breakpoints in your code.

The signature of the methods that you can use for preconversion, postconversion or custom converter scripts are:
The converter base class is Coveo.CES.DotNetConverterLoader.dll. You also need to reference the Coveo.CES.Interops.dll assembly to get the COMCoveoConverters.XXX object definitions. Both files are available in the [CES_Path]\Bin\ folder.

**Important:** In Visual Studio, do not worry that IntelliSense is not able to detect classes from the using declarations. When you will configure your script file (.css or .DLL) as a CES preconversion or postconversion script, it will work.

### 8.7.4.4.6.1 Sample C# Custom Converter

The following code is a sample of a C# custom converter.

```csharp
using Coveo.CES.DotNetConverterLoader;
using Coveo.CES.Interops.COMCoveoConvertersWrappers;

namespace TestDotNetConverter
{
    public class MyCustomConverter : CustomConverter
    {
        public override void RunPreConverter(PreConversion p_PreConversion, DocumentInfo p_DocumentInfo)
        {
            p_PreConversion.Trace("Hello, world!", SeverityEnumeration.SeverityNormal);
        }

        public override void RunPostConverter(PostConversion p_PostConversion, DocumentInfo p_DocumentInfo)
        {
            p_PostConversion.Trace("Hello, world!", SeverityEnumeration.SeverityNormal);
        }

        public override void RunCustomConverter(CustomConversion p_CustomConversion, DocumentInfo p_DocumentInfo)
        {
            p_CustomConversion.Trace("Hello, world!", SeverityEnumeration.SeverityNormal);
        }
    }
}
```

The .NET custom converters must inherit from the CustomConverter class, and implement a method named RunPostConverter that takes as arguments the objects that would normally be available as global variables in VBS scripts.

### 8.7.4.4.7 Applying a Global Conversion Script

When preconversion or postconversion scripts are available to CES (see "Adding a Preconversion Script" on page 460 and "Adding a Postconversion Script" on page 462), you can apply a conversion script to all documents of all
index sources. Only one global preconversion script and one global postconversion script can be applied to the index at a time.

**Note:** You can also apply one or more preconversion and postconversion scripts on every document in a specific source (see "Applying a Source Conversion Script" on page 465).

To apply a global conversion script

1. On the Coveo server, access the Administration Tool.
2. Select **Configuration > Converters**.
3. In the **Converter Managers** page, in the navigation panel on the left, click **Conversion Scripts**.
4. In the **Conversion Scripts** page:
   a. In the **Global Preconversion Script** and **Global Postconversion Script** drop-down lists, select the appropriate scripts.
   b. Click **Apply Changes**.

What's Next?

Rebuild all collections and sources of the index.

8.7.4.4.8 Applying a Source Conversion Script

When preconversion or postconversion scripts are available to CES (see "Adding a Preconversion Script" on page 460 and "Adding a Postconversion Script" on page 462), you can apply a conversion script to every documents of a specific source. Only one preconversion script and one postconversion script can be applied per source.
Notes:

- You can execute the conversion script on every document of every index source (see "Applying a Global Conversion Script" on page 464).

- CES 7.0.6424+ (February 2014) Once a preconversion, postconversion, or custom converter script (.NET, JScript, or VBScript) is applied to a source, you can modify and save the script file on the fly and it will be immediately and automatically reloaded and applied, even on an ongoing incremental refresh, full refresh, or rebuild of the source.

- CES 7.0.6607+ (April 2014) An entry in the CES Console and logs identifies preconversion and postconversion scripts applied during a rebuild, full refresh, or incremental refresh of a source. These log entries can be useful to help troubleshoot source issues caused by conversion scripts.

The log entries are in the form:

```
IMPORTANT|[yyyy-mm-dd]|[hh:mm:ss]|[n]|A [SourceAction] on source [SourceName] (with conversion script [ListOfPre&PostConversionScripts]) has been requested by coveo\[username].
```

Example: The following log entry shows that the MyPreconversionScript and MyPostconversionScript scripts were applied to the rebuild of the source FileShare1.

```
IMPORTANT|2014-09-16|15:02:54|0|A rebuild on source FileShare1 (with conversion script MyPreconversionScript, MyPostconversionScript) has been requested by coveo\crawlinguser.
```

To apply a source conversion script

1. On the Coveo server, access the Administration Tool.

2. Select Index > Sources and Collections.

3. In the Sources and Collections page:
   a. In the Collections section, select the collection that contains the source to which you want to apply a conversion script.
   b. In the Sources section, expand the appropriate source drop-down list, and then select Edit Conversion.
4. In the **Conversion Scripts** page for the source:
a. In the **Preconversion Scripts** or **Postconversion Scripts** drop-down list, select the appropriate script.

   **Note:** A script appears in the appropriate drop-down list only after being added to CES (see "Adding a Preconversion Script" on page 460 and "Adding a Postconversion Script" on page 462).

b. If the preconversion or postconversion script requires other parameters, for each parameter, click **Add Parameter** in the **Parameters** section, and then enter the name and value of the parameter.

c. Click **Apply Changes**. Note that it is possible to set parameters to scripts.

Once you apply the script to a source, on the script page, the source name will appear next to **Used By**.

### What's Next?

Rebuild the source.

### 8.7.4.4.9 Modifying How Documents Written in Unrecognized Languages Are Indexed

When a document is written in a language other than one of the supported languages, it is attributed the *Unknown* language status in the index. By default, CES indexes documents written in unknown languages only if their size is inferior to 4,096 bytes. However, it is possible to modify this behavior.

To modify the indexing of documents written in unrecognized languages

1. On the Coveo server, access the Administration Tool.
2. Access the **Converter Managers** page (**Configuration > Converters**).
3. In the navigation panel on the left, click **Languages**.
4. In the **Languages** page:

   ![Converter Managers](image)

   a. In the **Language Detection** section, select one of the following action to apply when the language of the document is registered as *Unknown*:
Use indexing failure action set for the document type

CES handles documents in unknown languages as corrupted documents whose content cannot be indexed—they are either rejected or indexed by reference depending on the **Indexing Failure Action** selected for this document type (see "Modifying How CES Handles a Document Type" on page 477).

**Reject the document**

CES does not index documents in unknown languages.

**Index**

CES indexes all documents in unknown languages.

**Index if document is smaller than X bytes**

CES indexes documents in unknown languages only if their size is inferior to the specified value in bytes.

b. Click **Apply Changes**.

8.7.4.4.10 Modifying Advanced Converter Parameters

You can modify advanced converter parameters to fine tune the CPU resources consumed by the converters:

**Summary Length**

Indicates the maximum number of words which can be extracted to form document summaries.

**Conversion Queue**

Indicates the number of documents which can be kept in the conversion buffer before the crawling process is stopped to avoid overloading the converters.

To modify advanced converter parameters

1. On the Coveo server, access the Administration Tool.
2. Select **Configuration > Converters**.
3. In the **Converter Managers** page, in the navigation panel on the left, click **Advanced**.
4. In the **Advanced** page:
a. In the **Summary Length** box, modify the maximum number of words allowed in summaries.

b. In the **Conversion Queue** box, modify the maximum number of documents allowed in the conversion queue.

c. Click **Apply Changes**.

### 8.7.4.4.11 About the Enhanced Quick View

The Coveo Platform has always included a Quick View feature. At indexing time, an HTML version of each indexed document can be created and included in the index to allow end users to preview the content of a search result without having to open its associated application.

The original Quick View is a simple HTML version of indexed documents that has low impact on index size and indexing performance and still allows end users to quickly locate searched terms in the document, find the information they are looking for, or validate that this is the document they are looking for. When the document contains images or is graphically rich, the original Quick View may not be a visually representative version of the original document.

The purpose of the enhanced Quick View is to provide an accurate representation of documents in their original form, including their layout, images, and formatting. The original Quick View remains available and is used as a fallback option when the enhanced Quick View generation fails for a given document.

The enhanced Quick View uses LibreOffice and PDF2HTMLEx third-party software to create more accurate representations of documents in various file formats. LibreOffice converts each document from its original format to PDF, and then PDF2HTMLEx converts the PDF to HTML (see "Installing the Enhanced Quick View Components" on page 472).

You can also use only LibreOffice to perform both the conversion from the original document format to PDF and from PDF to HTML. However, using PDF2HTMLEx to perform the PDF to HTML conversion generally produces better rendering.
Important: Creating an enhanced Quick View for a document requires significant server resources and adds a significant size to the index, particularly for graphically rich documents.

Be aware that using the enhanced Quick View can have the following impact:

- Increases the index size by a factor of 2 to 5 if all indexed documents use the enhanced Quick View (up to a factor of 10 when all documents are graphically rich such as PowerPoint documents).
- Increases time to index by a factor of 2 to 40 depending on the size and graphical content of documents.
- Increases the time it takes to open the Quick View in the search interface proportionally to the file size.
- PDF2HTMLEx does not officially support mobile devices and various issues such as performance ones can occur on some devices (see Mobile Devices).

It is therefore recommended to restrict the use of the enhanced Quick View to sources and document types for which it provides significant added value to your end users.

You can precisely control which file formats for which sources are converted with the original or the enhanced Quick View using one or more Document Type Sets assigned to one or more sources (see "Enhanced Quick View Deployment Overview" on page 471).

File formats supported by the enhanced Quick View:

- Microsoft Office (Word, Excel, PowerPoint, Publisher)
- Adobe PDF
- Microsoft Visio (2000-2013)
- Lotus Notes (for content indexed as RTF)
- Rich Text Format Documents (RTF)
- WordPerfect

Feature history

<table>
<thead>
<tr>
<th>CES version</th>
<th>Monthly release</th>
<th>Features</th>
</tr>
</thead>
<tbody>
<tr>
<td>7.0.6607</td>
<td>April 2014</td>
<td>Can now only use LibreOffice to perform the conversion from the original document directly to HTML.</td>
</tr>
<tr>
<td>7.0.6547</td>
<td>March 2014</td>
<td>Enhanced Quick View introduction in beta version</td>
</tr>
</tbody>
</table>

8.7.4.4.11.1 Enhanced Quick View Deployment Overview

The following procedure outlines the tasks that you must perform to deploy the enhanced Quick View.

Important: Generating enhanced Quick Views can significantly increase the index size and the time and
resources required to index converted documents.

It is therefore recommended to:

- Initially use the enhanced Quick View for one source containing a limited number of documents to convert.

- Evaluate the impact on your Coveo server:
  - Measure the index size increase.
  - Monitor time and server resources required to convert documents.

- When you understand the impact on your server, proceed to enable the enhanced Quick View on other sources.

To deploy the enhanced Quick View

1. Ensure that:
   a. Your Coveo server clearly meets the requirements for your index size.
   b. The hard disk where the index resides is far from being full.

2. Install the components required to create the enhanced Quick View (see "Installing the Enhanced Quick View Components" on page 472).

3. Consider creating a new document type set for the enhanced Quick View (see "Creating a Document Type Set" on page 477).

4. In a newly created or selected document type set, configure each file format for which you want to use the enhanced Quick View (see Modifying How CES Handles a Document Type).

   By default, the original Quick View is used.

5. Assign the modified document type set to one or more sources for which you want to have enhanced Quick Views (see "Modifying the Document Type Set Used by a Source" on page 481).

6. Ensure that the Generate a cached HTML version of indexed documents option is selected for the sources.

7. Rebuild one source at a time, starting with a source that indexes only a limited number of documents.

   **Note:** You can monitor the indexing and the conversion processes from the CES Console or from the source Status page.

8. In the search interface, if large Quick Views take too long to load, consider limiting the download size of Quick View files (see "Limiting the Quick View Size in Search Interfaces With the .NET Interface Editor" on page 546).

8.7.4.4.11.2 Installing the Enhanced Quick View Components

Generating enhanced Quick Views is done using third-party components. Before you can build or rebuild sources to include enhanced Quick Views in the index, you must install these components on your Coveo server.
To install the enhanced Quick View components

1. Using an administrator account, connect to the Coveo server where converters are running.

   By default, the converters are running on the Coveo Master server, but they can also be running on Coveo Mirror servers and dedicated Coveo Remote Converter servers. You must perform this procedure for each Coveo server where converters running.

2. Install LibreOffice:
   a. Download the LibreOffice installer (version 4.1+ is required).
   b. Run the LibreOffice installer, and then note the path where it is installed.

3. Install PDF2HTMLEx:
   a. Download the PDF2HTMLEx archive file.
   b. Decompress the PDF2HTMLEx archive file on the Coveo server in a path accessible to the user that runs the CES service.

   Example: Decompress the PDF2HTMLEx archive in the C:\Program Files\PDF2HTMLEx\ folder.

4. Access the CES Administration Tool.

5. Select Configuration > Converters.

6. In the navigation panel on the left, select Converter Managers.

7. In the Converter Managers page, in the Converter Managers list, click the converter for which you want to configure the enhanced Quick View.

8. In the page for the selected converter, in the Enhanced Quick View section:
a. In the **LibreOffice Path** box, specify the path to the LibreOffice executable in the form:

```
[LibreOffice_Path]\program\soffice.exe
```

**Example:** When LibreOffice 4.x.x win32 is installed in the default location, the path is:

```
C:\Program Files (x86)\LibreOffice 4\program\soffice.exe
```

b. In the **PDF2HTMLEx Path** box, specify the path to the PDF2HTMLEx executable in the form:

```
[PDF2HTMLEx_Path]\PDF2HTMLEx.exe
```

**Example:**

```
C:\Program Files (x86)\PDF2HTMLEx\PDF2HTMLEx.exe
```

c. Optionally, when you want to customize how the PDF2HTMLEx component operates, in the **PDF2HTMLEx parameters** box, change the command-line parameters that are passed to the PDF2HTMLEx executable for the Quick View conversion.

The recommended parameters are: 

```
--hdpi 48 --vdpi 48 --embed-external-font 0
```
**Tip:** To reduce the enhanced Quick View index footprint:

- Try adding `--embed-font 0` to disable font embedding and save about 100 KB per document. In the best case you may lose markup such as bold and italic, but in the case of a foreign language the whole document could be unreadable if the end-user computer does not have an appropriate font.

- Try adding `--hdpi 36 --vdpi 36` to further reduce the horizontal and vertical image resolutions expressed in dot per inch (DPI) when you can accept a little loss of image rendering quality.

- Try adding `--process-outline 0 --optimize-text 1 --embed-outline 0 --printing 0` to save about 20 KB per document.

Leaving the PDF2HTMLEx Options box empty will use the default values for all PDF2HTMLEx options. You can get the complete list of command-line options by running `PDF2HTMLEx.exe -h` in a Command Prompt window.

The following table provides a subset of PDF2HTMLEx command-line options that you can use to optimize the Quick View rendering quality versus file size.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>--zoom &lt;fp&gt;</code></td>
<td>zoom ratio</td>
</tr>
<tr>
<td><code>--fit-width &lt;fp&gt;</code></td>
<td>fit width to &lt;fp&gt; pixels</td>
</tr>
<tr>
<td><code>--fit-height &lt;fp&gt;</code></td>
<td>fit height to &lt;fp&gt; pixels</td>
</tr>
<tr>
<td><code>--hdpi &lt;fp&gt;</code></td>
<td>horizontal resolution for graphics in DPI (default: 144)</td>
</tr>
<tr>
<td><code>--vdpi &lt;fp&gt;</code></td>
<td>vertical resolution for graphics in DPI (default: 144)</td>
</tr>
<tr>
<td><code>--embed &lt;string&gt;</code></td>
<td>specify which elements should be embedded into output</td>
</tr>
<tr>
<td><code>--embed-css &lt;int&gt;</code></td>
<td>embed CSS files into output (default: 1)</td>
</tr>
<tr>
<td><code>--embed-font &lt;int&gt;</code></td>
<td>embed font files into output (default: 1)</td>
</tr>
<tr>
<td><code>--embed-image &lt;int&gt;</code></td>
<td>embed image files into output (default: 1)</td>
</tr>
<tr>
<td><code>--embed-javascript &lt;int&gt;</code></td>
<td>embed JavaScript files into output (default: 1)</td>
</tr>
<tr>
<td><code>--embed-outline &lt;int&gt;</code></td>
<td>embed outlines into output (default: 1)</td>
</tr>
<tr>
<td><code>--split-pages &lt;int&gt;</code></td>
<td>split pages into separate files (default: 0)</td>
</tr>
<tr>
<td><code>--process-nontext &lt;int&gt;</code></td>
<td>render graphics in addition to text (default: 1)</td>
</tr>
<tr>
<td><code>--printing &lt;int&gt;</code></td>
<td>enable printing support (default: 1)</td>
</tr>
<tr>
<td><code>--fallback &lt;int&gt;</code></td>
<td>output in fallback mode (default: 0)</td>
</tr>
<tr>
<td>Parameter</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>--embed-external-font</td>
<td>embed local match for external fonts (default: 1)</td>
</tr>
<tr>
<td>--font-format &lt;string&gt;</td>
<td>suffix for embedded font files (ttf,otf,woff,svg) (default: &quot;woff&quot;)</td>
</tr>
<tr>
<td>--override-fstype &lt;int&gt;</td>
<td>clear the fstype bits in TTF/OTF fonts (default: 0)</td>
</tr>
<tr>
<td>--heps &lt;fp&gt;</td>
<td>horizontal threshold for merging text, in pixels (default: 1)</td>
</tr>
<tr>
<td>--veps &lt;fp&gt;</td>
<td>vertical threshold for merging text, in pixels (default: 1)</td>
</tr>
<tr>
<td>--font-size-multiplier</td>
<td>a value greater than 1 increases the rendering accuracy (default:4)</td>
</tr>
<tr>
<td>--space-as-offset &lt;int&gt;</td>
<td>treat space characters as offsets (default: 0)</td>
</tr>
<tr>
<td>--tounicode &lt;int&gt;</td>
<td>how to handle TsoUnicode CMaps (0=auto, 1=force, -1=ignore) (default: 0)</td>
</tr>
<tr>
<td>--optimize-text &lt;int&gt;</td>
<td>try to reduce the number of HTML elements used for text (default:0)</td>
</tr>
<tr>
<td>--bg-format &lt;string&gt;</td>
<td>specify background image format (default: &quot;png&quot;)</td>
</tr>
<tr>
<td>--clean-tmp &lt;int&gt;</td>
<td>remove temporary files after conversion (default: 1)</td>
</tr>
<tr>
<td>--data-dir &lt;string&gt;</td>
<td>specify data directory (default: &quot;&quot;)</td>
</tr>
<tr>
<td>-h,--help</td>
<td>print usage information</td>
</tr>
</tbody>
</table>

d. Click **Apply Changes**.

**What's Next?**

- Consider creating a new document type set for the enhanced Quick View (see "Creating a Document Type Set" on page 477).

  OR

- In the selected document type set, configure each file format for which you want to use the enhanced Quick View (see Modifying How CES Handles a Document Type).

**8.7.4.5 Administration Tool - Document Types Menu**

As a Coveo Platform administrator, you can access this menu to define certain group of document types (PDF, HTML, etc.) to be indexed by a source and set how CES should index each file type.

**8.7.4.5.1 What Are Document Type Sets?**

A document type set defines a group of document types (PDF, HTML, etc.) to be indexed by a source and includes information on how CES should index each file type. You can assign a different document type set to each source.

**Example:** You can index PowerPoint documents in the Marketing source but not in the Human Resources source.

*www.coveo.com*
8.7.4.5.2 Creating a Document Type Set

Consider adding a document type set when you want to customize the list of file types to index or when you want to fine tune how one file type will be indexed. You can assign a document type set to one or more sources.

To create a new document type set

1. On the Coveo server, access the Administration Tool.
2. Access the Document Type Sets page (Configuration > Document Types).
3. In the Document Type Sets page, click Add.
4. In the Add Document Type Set page:
   a. In the Name box, enter a name to identify the document type set.
   b. In the Description box, enter a description of the document type set to help identify its purpose.
5. Click Save.

What's Next?

At this point, the new document type set is a copy of the Default one that you need to customize (see "Modifying How CES Handles a Document Type" on page 477).

You will then associate the document type set to the desired source (see "Modifying the Document Type Set Used by a Source" on page 481).

8.7.4.5.3 Modifying How CES Handles a Document Type

Document types describe how CES handles each file encountered during indexing. In a document type set, you can add or remove document types and for each document type, you can configure what CES does with files of this type.

To modify how CES handles files of a specific document type

1. On the Coveo server, access the Administration Tool.
2. Access the Document Type Sets page (Configuration > Document Types).
3. In the Document Type Sets page, click the document type set that you want to modify.
4. In the Document Types page, click the document type that you want to modify.
5. In the configuration page for the selected document type:
a. Modify the appropriate parameters:

**File Extensions**

Enter one or more file extensions, separated by a semicolon, corresponding to the document type.

**Example:** For help files: `.chm;.hlp`

**Action**

Select the appropriate indexing action taken by CES for this document type:

**Index entire document**

Indexes the whole content of the document. This is called indexing by content.

**Index file information only**

Only indexes file metadata. This is called indexing by reference.
Reject document

Does not index the document.

Indexing Failure Action

Select the action taken when the document is corrupted and cannot be indexed:

Index file information only

Only indexes file metadata.

Reject document

Does not index the document.

Converter

Select one of the two options to specify which converter to use to process documents that belong to the document type.

Use a default converter

Select to use one of the built-in CES converters, and then select the desired converter in the drop-down list. Select Detect to let CES automatically select the appropriate converter based on the detected file type.

Use an open converter

Select to rather use an open converter, and then select the appropriate open converter in the drop-down list.

Content Types

Optionally enter the type of content returned by custom connectors for this document type.

Example: binarydata.

sysfiletype Field Value

Select the value for the sysfiletype field.

Use the value set by the converter

By default, select this option to let the selected converter set the field value.

Use this value

Select to set a custom value, independent of the converter, and then enter the desired value in the box.

Quick View

Select how the cached HTML version for indexed document of this type will be generated (see “About the Enhanced Quick View” on page 470):

- Default
- LibreOffice and PDF2HTMLEx
- LibreOffice Only

Note: The Quick View option is available starting from the CES 7.0.6547 March 2014 monthly release.
Default

Select to create the cached HTML version with the original Quick View feature.

The original Quick View is a simple HTML version that has low impact on index size and indexing performance, but still allows end users to quickly locate searched terms in the document. When the document contains images or is graphically rich, the original Quick View may not be a visually representative version of the original document.

It is recommended to select Default for document types that contain only text, or contain graphical content that is not required to review the document meaning.

LibreOffice and PDF2HTMLEx

Select to create enhanced Quick Views for this document type using LibreOffice to convert documents to PDF format, and PDF2HTMLEx to convert the PDF to HTML format. This option produces the most accurate HTML reproduction of the original documents, but requires significant server resources and significantly increases the index size.

It is recommended to select LibreOffice and PDF2HTMLEx only for document types with important and meaningful graphical content such as Microsoft PowerPoint document.

LibreOffice Only

Select to create enhanced Quick Views for this document type, but only using LibreOffice to convert documents directly to HTML format. This option produces a less accurate HTML reproduction of the original documents, but also requires less server resources and does not increase the index size as much.

It is also recommended to select LibreOffice Only only for document types with important and meaningful graphical content. Select LibreOffice Only over LibreOffice and PDF2HTMLEx when you can compromise on the HTML reproduction quality to reduce requirements on server resources.

Notes: When LibreOffice and PDF2HTMLEx or LibreOffice Only is selected:

- If the conversion for a given document fails, the original Quick View is created as a fallback option and will be available for the corresponding search results in the search interface.
- If a PDF document is indexed, PDF2HTMLEx is used to generate the HTML.

Options

When indexing attachments, index the parent document

Select this check box to index email attachments or archive documents (ex.: documents in .zip files) with their parent document. This option is not selected by default.

Inherits source options

Select this check box to apply the Disable document summarization and Open results with cached version options selected for the parent source to the document type. This option is selected by default. Clear this check box to customize the following two options.
Disable document summarization

Select this check box to apply a different Disable document summarization option to the document type than the one selected for the parent source. To make this option available, clear the Inherits source options check box. The Disable document summarization option is not selected by default.

Open results with cached version

Select this check box to force search result items for this document type to open in a Quick View with a cached version, independently from the Open results with cached version option set for the parent source. To make this option available, clear the Inherits source options check box. The Open results with cached version option is not selected by default.

Title Selection Sequence

Use the arrows to set the order of actions taken to attempt to set the document title independently from the parent source. When CES fails to extract a title using the first option, it proceeds to the second one and so on. The title appears in the search result list. To make this option available, clear the Inherits source options check box.

Title Metadata Name

Uses a different Title Metadata Name to index the document type than the one selected for the parent source. To make this option available, clear the Inherits source options check box.

b. Click Apply Changes.

What's Next?

Ensure this modified document type set is associated to the appropriate source or sources (see "Modifying the Document Type Set Used by a Source" on page 481).

8.7.4.5.4 What Is the Difference between Indexing by Reference and Indexing by Content?

When CES indexes a document by reference, it only records the file information (path, filename, and metadata). The purpose of indexing by reference is to be able to see and open documents in the search interface even when their type is not supported by converters or IFilters. Indexing by reference saves index space but of course, limits the precision of results because only the metadata and paths of documents can be queried.

Example: When scanned documents include useful metadata such as title, subject, description, date etc., you can index them by reference so that they can appear in search results for queries matching the metadata content.

When CES indexes a document by content, it records the file information and indexes the text content of the file.

Note: CES converters support several document types. You can index other document types using open converters (see "Adding an Open Converter" on page 459) or using IFilters (see "What Are IFilters?" on page 482).

8.7.4.5.5 Modifying the Document Type Set Used by a Source

You can create a specific document type set and associate it to a source to control how the source handles particular document types when indexing files.
To modify the document type set used by a source

1. On the Coveo server, access the Administration Tool.
2. Select Index > Sources and Collections.
3. In the Sources and Collections page:
   a. In the Collections section, select the collection that contains the source that you want to modify.
   b. In the Sources section, expand the drop-down list for the source that you want to modify, and then select Edit Document Types.
4. In the Document Types page corresponding to the selected source:
   a. In the Document Type Set drop-down list, select the appropriate document type set.
   b. Click Apply Changes.

8.7.4.5.6 What Are IFilters?

IFilters are third-party converters used by CES to index document types not supported by its default or open converters. Adding IFilters to a document type set is a quick and easy way to increase the number of document types indexed by CES. However, IFilters produce larger files and poorer resolutions than CES converters.

8.7.4.5.7 Applying IFilters to Document Types

IFilters are third-party converters used by CES to index document types not supported by its default or open converters.
To apply an IFilter to a document type set

**Note:** IFilters must be applied to each document type set individually.

1. On the Coveo Master server, download the desired IFilters from a source such as www.ifiltershop.com.
2. Install the IFilters on the server.
3. Access the Administration Tool.
4. Select Configuration > Document Types.
5. In the Document Type Sets page, click the document type set for which you want to apply the IFilter to a document type.
   
   All IFilters installed on the server are associated with their corresponding document type for this document type set.

   **Note:** You can remove IFilter mappings for this document type set by clicking Unload IFilter Mapping.

What's Next?

Ensure that the source containing the document types converted by the IFilters uses the document type set that you modified.

8.7.4.6 Administration Tool - Languages Menu

Use the Languages menu to specify languages among supported ones contained in the default language set for CES to consider when indexing a source.

8.7.4.6.1 Adding and Configuring a Language Set

The Coveo Platform supports many languages. The default language set that Coveo Enterprise Search (CES) uses to manage languages contains all supported languages. You can create one or more other language sets to specify languages to consider.

**Example:** You know that your index exclusively contains documents written in English and French and do not want CES to attempt to detect other languages. You can create a language set for these two languages and assign it to your sources.

**Tip:** When your indexed content includes non language expressions (such as databases with various technical content or programing code sample) it is a good practice to use a language set that only includes languages you know are present in indexed content. Otherwise some strings could be mistakenly detected as belonging to an unexpected foreign language, and this foreign language be added to the syslanguage field for the document containing the string. This unexpected language could appear in a Language facet.
To add and configure a language set

1. On the Coveo server, access the Administration Tool.

2. Select Configuration > Languages.

3. In the Active Language Sets page:
   - To create a language set that initially includes all languages:
     a. Click Add.
     b. In the Add a Set of Active Languages page:
        i. In the Name box, enter a name for your new language set.
        ii. In the Description box, optionally enter a description for your new language set to help you identify the purpose of the language set.
        iii. Click Save.
   - To start from an existing language set, select the check box for language set from which you want to start, and then click Duplicate.

4. Back in the Active Language Sets page, click the newly created language set.

5. In the Active Languages page for the selected language set:
   a. Select the check box of one or more languages for which you want to change the state.
   b. Click Enable or Disable to respectively add or remove the language from the set.
c. When you are editing a duplicated language set, in the navigation panel on the right, click General, and then adapt the Name and Description for this new language set.

What's Next?
Assign the new language set to one or more sources (see "Assigning a Language Set to a Source" on page 485).

8.7.4.6.2 Assigning a Language Set to a Source

When you have one or more custom language set (see "Adding and Configuring a Language Set" on page 483) you can assign them to one or more sources so that CES only considers specific languages when indexing a source.

To assign a language set to a source

1. On the Coveo server, access the Administration Tool.
2. Select Index > Sources and Collections.
3. In the Sources and Collections page:
   a. In the Collections section, select the collection containing the source that you want to modify.
   b. In the Sources section, select the source.
4. In the navigation panel on the left, select Active Languages.
5. In the Active Language Set drop-down list, select the language set that you want to assign to this source.

What's Next?
Rebuild the source (see "Applying an Action to a Collection or a Source" on page 283).
8.7.4.6.3 Chinese Japanese Korean Thai Language Improved Relevance

The Coveo Platform 7 has always supported Chinese, Japanese, Korean, and Thai (CJKT), but now offers improved relevance for these languages.

These languages do not use spacing characters to separate words. Previously, Coveo Enterprise Search (CES) was indexing each character separately as if it was a word and used pairs of such characters to perform retrieval. This indexing method allows end users to find content, but was not optimal for example for search results precision and ranking.

With the new indexing method, Coveo Enterprise Search (CES) uses proven language aware word tokenizers to identify and separate expressions in individual groups of inseparable characters referred to hereafter as CJKT words. Each CJKT word is then indexed as normal words. The meaning of CJKT words is thus preserved and ranking is done on words rather than on individual characters, allowing for improved relevance.

Example: You can enter Chinese, Japanese, Korean, or Thai keywords in the search box to get relevant documents in search results and see highlighted CJKT keyword occurrences in the search results title and excerpt such as in the following Chinese example.

Notes:
- CES 7.0.6424+ (February 2014) Improved relevance for Thai.
- CES 7.0.6547+ (March 2014) New index created use the new improved relevance CJKT indexing method.

When you upgrade CES from a version prior to CES 7.0.6547 to a CES 7.0.6547+ version, an existing index will by default continue to use the original CJKT indexing method. If you want to switch to the new CJKT indexing method, contact Coveo Support for assistance.

In the examples presented below, a group of similar uppercase letters (ex.: TTT) represents a CJKT word, while a group of different lowercase letters (ex.: abc) represents a non-CJKT word or term.
**Example:** The simplified Chinese expression for Coveo supports many languages is decomposed as follows:

<table>
<thead>
<tr>
<th>Original expression:</th>
<th>coveo支持多国语言</th>
</tr>
</thead>
<tbody>
<tr>
<td>Represented by:</td>
<td>abc TTTUUU</td>
</tr>
<tr>
<td>where:</td>
<td>abc stands for coveo</td>
</tr>
<tr>
<td></td>
<td>TTT stands for 支持 (support)</td>
</tr>
<tr>
<td></td>
<td>UUU stands for 多国语言 (multilingual)</td>
</tr>
</tbody>
</table>

**Supported feature** | **Description**
--- | ---
**Indexing** | Automatic detection of CJKT content based on each language specific Unicode character sets and encodings. As are words for other languages, CJKT words are indexed to identify in what documents they appear, and where they appear in each document.

**Search** | At query time, a CJKT expression is split into CJKT words and the search results present all documents containing all CJKT words. In the search interface, the searched CJKT words are highlighted in search results title and excerpt. End-users can search for CJKT words mixed with non-CJKT words or terms.

**Example:**

<table>
<thead>
<tr>
<th>Typed query:</th>
<th>abcTTTUUDef</th>
</tr>
</thead>
<tbody>
<tr>
<td>Transformed query:</td>
<td>(abc TTT UUU def)</td>
</tr>
</tbody>
</table>

**Note:** Returned documents are ranked using the same process and criteria as for other languages (see "Administration Tool - Ranking Menu" on page 317).
<table>
<thead>
<tr>
<th>Supported feature</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Prefixes and operators</td>
<td>In the search box of Coveo search interfaces, end-users can use search prefixes and operators with CJKT expressions. The Boolean operators must be spelled in English (AND, OR, NEAR, NOT).</td>
</tr>
</tbody>
</table>
| **Example**: End-users can use the OR operator between a word and a CJKT expression: | **Typed query**: abc OR TTTUUU  
**Transformed query**: (abc OR (TTT UUU))                                                                                           |
| **Examples**: End-users can use the NEAR operator between a word and a CJKT expression: | **Typed query**: abc NEAR TTTUUU  
**Transformed query**: (abc NEAR "TTT UUU")  
**Typed query**: r-cTTTUUU NEAR def  
**Transformed query**: ("r c TTT UUU" NEAR def)                              |
| **Note**: The NEAR operator supports matching a word or a phrase, but not a subexpression.                                           |
| **Examples**: End-users can use the NOT or minus operator that will expand to an exact phrase match when preceding a CJKT expression: | **Typed query**: NOT TTTUUU  
**Transformed query**: NOT "TTT UUU"  
**Typed query**: -TTTUUU  
**Transformed query**: -"TTT UUU"                                                                                       |
| **Examples**: While stemming does not apply to CJKT, end-users can still use the exact match plus (+) or number sign (#) operators in front of a CJKT expression to expand the expression as an exact phrase. The operator will be stripped. | **Typed query**: +TTTUUU  
**Transformed query**: "TTT UUU"  
**Typed query**: #TTTUUU  
**Transformed query**: "TTT UUU"                                                                 |
## Supported feature

<table>
<thead>
<tr>
<th>Description</th>
</tr>
</thead>
</table>
| **Phrase search** | In the search box of Coveo search interfaces, end-users can search for a specific CJKT phrase. The phrase semantic will be preserved.  
**Example:** End-users can use double quotes to delimit an expression to exactly match:  
**Typed query:** `abc"TTTUUUdef"`  
**Transformed query:** `abc "TTT UUU def"`  
Non-word characters generate an exact phrase of surrounding characters.  
**Example:** The presence of the dash (−) forces a conversion to an exact phrase match:  
**Typed query:** `TTTUUVVV`  
**Transformed query:** `"TTT UUU VVV"`  |
| **Thesaurus** | A Coveo administrator can enter CJKT expressions in thesaurus entries to expand queries (see "Adding Thesaurus Entries From the Administration Tool" on page 332).  
**Note:** CJKT thesaurus entries are applied on CJKT words so a CJKT expression and its CJKT words are considered equivalent.  
**Example:** Entering `TTTUUVV` or `TTT UUU` in a thesaurus entry has the same effect. |
| **Field queries** | Thai expressions can be used in field queries. Matches within fields are more precise, because they are converted to exact phrase matches.  
**Examples:**  
**Typed query:** `@field=abcTTTUUU`  
**Transformed query:** `@field="abc TTT UUU"`  
**Typed query:** `@field=(abc,TTTUUVV)`  
**Transformed query:** `@field=(abc, "TTT UUU")`  |
| **Stop words** | A Coveo administrator can include CJKT words as stop words (see "Configuring the Index to Ignore Stop Words in Queries" on page 124). |
| **Did you mean** | The Word Corrector Lexicon (WCL) supports CJKT words so mistyped CJKT expression can lead to *Did You Mean* suggestions at query time. |

**Note:** The use of wildcards is not supported for Chinese, Japanese, Korean, and Thai.
8.7.4.7 Administration Tool - Fields Menu

In the Coveo unified index, fields are containers of structured data extracted for each document from each repository. Each field provides a single type of information about a document.

**Examples:**

- When you index emails, the `systo`, `sysfrom`, and `sysdate` fields respectively indicate the recipients, author, and date of an email message.

- When indexing Microsoft Word or PDF files from a file system, the `systitle`, `sysauthor`, and `sysdate` fields respectively indicate the title, author, and creation/modification date of the document.

- When you index Salesforce content, the `syssfaccount`, `syssfamount`, and `syssfcontact` fields respectively indicate the account, amount, and contact associated with an sales opportunity.

By default, CES indexes common system and repository-specific fields. You can create custom fields sets (see "Adding a Field Set" on page 491) to which you add custom fields to include more business logic metadata into the index (see "Adding or Modifying Custom Fields" on page 494).

You can use fields to:

- Create facets allowing end-users to easily refine results based on the field content (see "Adding or Customizing a Facet With the .NET Interface Editor" on page 576).

- Include field labels and values in search results (see "Adding Display Fields to Search Results With the .NET Interface Editor" on page 620).

- Sort search results based on the field content (see "Adding Sort Criteria With the .NET Interface Editor" on page 624).

- Configure fields to be searchable (see "Adding Search Fields With the .NET Interface Editor" on page 623).

8.7.4.7.1 What Is the Difference between Built-In and Custom Fields?

Built-in fields are provided by CES. They are the most common system, SharePoint, Microsoft Exchange and Lotus Notes fields. Whereas, custom fields are created by Coveo administrator to index other types of organized content (ex.: a custom SharePoint list column). Custom fields can be added and removed at any time, while built-in fields can only be modified.

8.7.4.7.2 What Are Field Sets?

A field set is a group of fields to be populated with values from corresponding metadata available on documents of a given source. The purpose of field set is to leverage structured content of a repository to deploy more feature-rich search interfaces with relevant facets, sort criteria, and display fields.

The `Default` field set includes standard built-in generic and repository-specific CES fields.

More connectors progressively come with a field set import file defining fields for all default metadata available for a repository type. The field set import files are available from the `[CES_Path]\Bin\` folder and the file name is in the following format: Coveo.CES.CustomCrawlers.[ConnectorName].FieldSet.xml. When a field set import file is available for a connector, it is a best practice to create a field set starting with importing the content of this file to
easily get all default fields that can immediately be used to create facets, sort criteria, and display fields (see "Exporting and Importing a Field Set" on page 492).

You can create custom field sets that are copies of the Default field set (see "Adding a Field Set" on page 491) but in which you can modify the properties of built-in fields and to which you can add custom fields to map specific metadata values from one or more repositories (see "Adding or Modifying Custom Fields" on page 494). You then assign a custom field set to one or more sources for which it was created (see "Modifying the Field Set Used by a Source" on page 498).

Example: You index a Sitecore website and want to index several business logic metadata from the website. You create a custom field set named My Sitecore Fields to which you add a bunch of custom fields for each of the Sitecore metadata that you want to index. You associate the custom field set to your Sitecore source.

8.7.4.7.3 Adding a Field Set

A new field set is a copy of the Default one (see "What Are Field Sets?" on page 490). You typically create a field set when you want to modify parameters of built-in fields and/or add custom fields to customize how CES manages metadata for one or more specific sources. You then assign the custom field set to the appropriate source or sources. Each source uses only one field set.

To add a field set

1. On the Coveo server, access the Administration Tool.
2. Select Configuration > Fields.
3. In the Fields Sets page, click Add.
4. In the Add Fields Set page:
a. In the **Name** box, enter a name to identify the field set.

   **Example:** You are creating a field set for Salesforce content and name the field set **My Salesforce Organization Custom Fields**.

b. In the **Description** box, optionally enter a description to help you remember the purpose of the field set and details about what you customized.

c. Click **Save**.

**What's Next?**

Add custom fields to your new field set (see "Adding or Modifying Custom Fields" on page 494) or modify existing built-in fields, and then associate the field set with the source(s) for which it was created (see "Modifying the Field Set Used by a Source" on page 498).

**8.7.4.7.4 Exporting and Importing a Field Set**

Creating a bunch of custom fields for a repository can be tedious. Once it is done in one Coveo server, you can export the corresponding field set to an XML file and import the file in another Coveo server.

This export/import process is particularly useful when you want to duplicate field sets between development, staging, and production environments. You can also create a new field set by importing a default XML field set file distributed with CES for various connectors.

**Note:** Several connectors come with a field set import file defining fields for all default metadata available for a repository type. The field set import files are available from the `[CES_Path]\Bin\` folder and the file name is in the following format:

```
Coveo.CES.CustomCrawlers.[ConnectorName].FieldSet.xml
```

When a default field set file is available for a connector, it is a best practice to create a field set starting with importing the content of this file to easily get all default fields that can immediately be used to create facets, sort criteria, and display fields. You can later add fields for custom metadata.

**To export a field set**

1. Using an administrator account, connect to the Coveo server that contains the field set to export.
2. Access the Administration Tool.
3. Select **Configuration > Fields**.
4. In the **Fields Sets** page, select the check box for the field set that you want to export, and then click **Export**.

   The exported file name is **FieldsSetsExport.xml**.

5. In the folder where your browser downloaded the file, using a text editor, open the exported XML file and copy its content.
To import a field set

1. Using an administrator account, connect to the Coveo server in which you want to import a field set.

2. Using a text editor, open and copy the content of the field set file that you want to import:
   - An exported field set file.
   - An appropriate out-of-the-box [CES_Path]\Bin\Coveo.CES.CustomCrawlers [ConnectorName].FieldSet.xml field set file.

3. On the Coveo server to which you want to import a field set, access the Administration Tool.

4. Select Configuration > Fields.

5. In the Fields Sets page, click Import.

6. In the import Fields Sets page, paste the content of an exported field set XML file or of an out-of-the-box field set import file in the Exported field sets list XML file content box, and then click Apply Changes.

What's Next?

Assign the field set to the appropriate sources (see "Modifying the Field Set Used by a Source" on page 498).

Add or adapt fields for custom metadata (see "Adding or Modifying Custom Fields" on page 494).
8.7.4.7.5 Adding or Modifying Custom Fields

Index fields can contain metadata extracted from structured content of crawled repositories. Field parameters determine to which metadata a field is mapped and how it can be used. You can add or modify custom fields to index additional information not covered by the built-in Coveo fields.

**Example:** You can index a custom SharePoint column called Department by adding a corresponding custom field.

**Notes:**
- **CES 7.0.7022+ (September 2014)** The index automatically processes existing field configuration changes such as allowing faceted search on a field. This process can take a few to several minutes for a large index so you will not immediately see the effect.
- **CES 7.0.6942– (August 2014)** When you change the configuration of an existing field, you must rebuild sources that are using this field.

To add custom fields

1. On the Coveo server, access the Administration Tool.
2. Select **Configuration > Fields**.
3. In the **Field Sets** page, click the field set to which you want to add or modify a field.
4. In the navigation panel on the left, select **Custom Fields** and then:
   - Click **Add** to create a new custom field.
   - OR
   - Click an existing custom field to modify it.
5. In the **Add a Custom Field** page:
In the **Name** box, enter a name to identify the custom field. The field name must be made of 1 to 64 characters only from the a-z, A-Z, and 0-9 ranges and must not start with a number. Field names are case insensitive.

**Note:** When the **Metadata Name** (see below) is left empty and the **Name** exactly matches a metadata name defined in the crawled repository, the content of the metadata is automatically copied to the index field for each crawled document containing this metadata. This is an easy way to map a repository metadata to an index field.

You can set a **Name** to be different from the **Metadata Name** to help you understand the origin of the field.

**Example:** You can use a prefix to identify all custom fields from a given repository. You create all custom fields for metadata from a Jive site with the jive prefix. For the Jive creationDate metadata, you create the jivecreationdate custom field.

**Note:** This name is used during field queries in the form @fieldname=fieldvalue.

In the **Type** section, select the option for the type of value accepted by the field.

Four types are available:

**String**

The field accepts series of characters without mathematical value. Usernames and passwords are string parameters.

**Numeric**

The field accepts integer numbers. The size of a document in bytes is a numeric value.
**Date/time**

The field accepts series of characters and numbers representing a date. The modification date of a document is a date/time value.

**Floating Point**

The field accepts numbers with fractions (ex.: 10.031).

c. In the Metadata Name box, enter the name of the metadata to which you want to map this field.

**Important:** Ensure to type the metadata name exactly as it is spelled in the crawled repository.

As mentioned above, you can leave this box empty in which case CES rather use the Name to attempt mapping to a metadata name.

d. In the Default Value box, enter the value indexed when a field is empty. This value must be the same as the field type.

**Example:** When the value of the Department field is empty, the default value, String, is indexed.

e. For Date/time type fields only, in the Date Format box, enter the format of the date in the metadata.

f. In the Option section, select the appropriate options:

**Include for field queries**

The content of the field can be queried using the format @fieldname=fieldvalue. This option is selected by default.

**Example:** The query @sysauthor=John returns documents whose author is John.

**Include for free text queries**

The content of the field can be queried using free text. This option is not selected by default and is available only if the field type is String.

**Example:** If free text queries are allowed on @sysauthor, documents returned by @sysauthor=John are also returned by John; however, the query John also returns documents containing the word John in their content, not only in the sysauthor field.

**Allow faceted search on this field**

The content of the field can be used to create a facet to form query refinement groups. This option is not selected by default and is available only if the field type is String.

**Example:** When the Allow faceted search on this field option is selected for the @sysauthor field, you can create an Author facet allowing users to refine results based on document authors.

**Create a smart date field** CES 7.0.5785+ (August 2013)

A new field is created containing the date of the original field but decomposed in values for the day, week, month, quarter, and year relative to January 1, 1900. The name of the new field is the original field name to which the SmartFacet suffix is appended. This field is useful to create more intuitive date
facets and charts.

Example: The original MyDate field contains 2013-02-24 and the new MyDateSmartFacet field contains D41329;W5904;M1357;Q452;Y113.

Allow faceted search on a field containing multiple values

The content of the multi-value field can be used to create a facet to form query refinement groups. The semicolon separated multiple values of the field are considered individually. This option is not selected by default and is available only if the field type is String.

Example: The multi-value @syslanguage field contains French;English for a document. When the Allow faceted search on a field containing multiple values option is selected, in the Language facet based on this field, this document counts twice (for the French and English items) rather than only once for the French;English item.

Allow to sort query results by this field

The content of the field can be used to sort search results. This option is not selected by default but is available for all field types.

Important: Adding sorting fields has an impact on the index size and performance. It is recommended to select the Allow to sort query results by this field option only for fields that you are planning to use to sort by in search interfaces.

Example: If @sysdate is used to sort results, the Sort by Date function (allowing to sort documents by modification date) is available in the search interface.

Set as display field

Selected by default to make the field visible in the Index Browser and available from the Interface Editor for inclusion as a Display Field in search results. Consider clearing unused fields to minimize the search results download size at query time. You can change this selection later.

g. Click Save.

Note: CES 7.0.7711+ (June 2015) When the field Name you entered matches the name of a custom or system field alias, you get the following error message:

This name is already used.

What’s Next?

CES 7.0.6942– (August 2014) Rebuild the sources using the field set containing the new or modified field(s).

CES 7.0.7022+ (September 2014) Depending on the modifications you have made:

- When you only modified the Options section selection for existing fields, you no longer need to perform source rebuilds.
Note: The index automatically processes the field configuration change(s). This process can take a few to several minutes for a large index so you will not immediately see the effect.

- When you add new fields or perform actions on existing fields such as modifying their name or changing their metadata name, you still need to rebuild the sources using the field set containing those fields.

8.7.4.7.6 Modifying the Field Set Used by a Source

A field set is a group of fields which indicates how CES should index the structured content of a repository. Field sets determine what field queries are allowed (ex.: `@sysauthor=John`). Note that each source can be indexed using a different field set to reflect its specificities.

To modify the field set used by a source

1. On the Coveo server, access the Administration Tool.
2. Access the Sources and Collections page (Index > Sources and Collections).
3. In the Sources section, expand the appropriate source drop-down list, and then select Edit Fields.

4. In the Fields page corresponding to the source:
   a. In the Field Set drop-down list, select the appropriate field set.
   b. Click Apply Changes.
8.7.4.7.7 Specifying a Date Format

Date formats are extracted using a string of values which indicates the position of the year, month, day, hours, minutes and seconds (note that the time in hours, minutes and seconds is optional).

**Example:** 05-31-2007 7:34:11 PM is extracted using `%m-%d-%Y %H: %M: %S %p` and 2007/5/31 7h34 PM is extracted using `%Y/%m/%d %h%M %p`.

The following table describes the string formats that you can use to extract date and time values.

<table>
<thead>
<tr>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>%Y</code></td>
<td>Four-digit year (ex: 2007)</td>
</tr>
<tr>
<td><code>%y</code></td>
<td>Two-digit year (ex: 07)</td>
</tr>
<tr>
<td><code>%m</code></td>
<td>Two-digit month (handles one-digit months, ex: 2007/05/31 or 2007/5/31)</td>
</tr>
<tr>
<td><code>%o</code></td>
<td>Three-letter month (ex: jan, may)</td>
</tr>
<tr>
<td><code>%d</code></td>
<td>Two-digit day (handles one-digit days, ex: 2007/05/01 or 2007/5/1)</td>
</tr>
<tr>
<td><code>%H</code></td>
<td>Two-hour (handles two-hour hours, ex: 12:30 or 4:30)</td>
</tr>
<tr>
<td><code>%M</code></td>
<td>Two-digit minute (ex: 4:02)</td>
</tr>
<tr>
<td><code>%S</code></td>
<td>Two-digit second (ex: 4:02:20)</td>
</tr>
<tr>
<td><code>%p</code></td>
<td>AM/PM detector</td>
</tr>
<tr>
<td><code>%G</code></td>
<td>Time zone (UTM)</td>
</tr>
</tbody>
</table>

8.7.4.7.8 Adding a Field to Search On

You may need to add which fields are available to search on in the .NET search interface Advanced Search page to help end-users refine queries without having to enter operators or field queries. Before doing that, you must ensure that the fields are set as Field Queries in the index.

To add a field to search on in the Advanced Search page

1. On the Coveo server, access the Administration Tool.
2. Select Configuration > Fields.
3. In the panel on the left, select the field set containing the field for which you want to control the availability to search on.
4. In the page that appears, locate the field that you want to use to search on, and then click the corresponding Field Queries check box.
Notes:

- You can also select Free Text Queries so that end-users can also query the content of the field using free text queries.
- Review the Metadata Name column to identify the original metadata from which the field value is extracted.

5. Click Apply changes.

What's Next?

Using the .NET Interface Editor, customize the search fields available in the .NET search interface Advanced Search page to help end-users refine queries without having to enter operators or field queries (see "Adding Search Fields With the .NET Interface Editor" on page 623).

8.7.4.7.9 Adding a Facet Field

You may need to control which fields are available to group on, so that you can use them to create facets in a .NET search interface (see "Adding or Customizing a Facet With the .NET Interface Editor" on page 576).

Some fields may contain more than one value for a given indexed document. You can set a field to be a Multi-value Facet to instruct CES to process multiple values independently.
Example: The `syslanguage` field is set to be a Multi-value Facet by default. When a document contains both English and Romanian content, in the **Language** facet, the document is included in the number of occurrences for both the **English** and **Romanian** facet items.

If `@syslanguage` was not set to be a Multi-value Facet, in the **Language** facet, the document occurrence would appear in the **English;Romanian** facet item, because the values of the field would be considered inseparable.

**Note:** CES only recognizes field values as independent when they are isolated by a value separator. The default separator (:) is used for all built-in fields. Other repositories such as databases or in-house applications can use different separators—refer to the documentation provided with the repository.

To add a facet field:

1. On the Coveo server, access the Administration Tool.
2. Select **Configuration > Fields**.
3. In the panel on the left, select the field set containing the field for which you want to control the availability to group on.
4. In the page that appears:
a. Select the **Facet** check box for field that you want to use to group on.

   **Note:** Review the **Metadata Name** column to identify the original metadata from which the field value is extracted.

b. Select the **Multi-value Facet** check box for fields that CES must considered as containing multiple independent values.

c. Click **Apply changes**.

**What's Next?**

- **CES 7.0.6942—(August 2014)** When you make an existing field a facet field, you must rebuild sources that are using a field set containing this field.

- **CES 7.0.7022+ (September 2014)** The index automatically processes the changes without a rebuild.

- Using the .NET Interface Editor, create a custom facet using this new facet field to help end-users refine queries in a .NET search interface (see "Adding or Customizing a Facet With the .NET Interface Editor" on page 576).

**8.7.4.7.10 Adding a Sorting Field**

You may need to add other sorting criteria so that end-users can more conveniently sort search results in the search interface.
Important: Adding sorting fields has an impact on the index size and performance. It is recommended to select the Sort check box only for fields that you are planning to use to sort by in search interfaces.

To add a sorting field

1. On the Coveo server, access the Administration Tool.
2. Select Configuration > Fields.
3. In the panel on the left, select the field set containing the field for which you want to control the availability to sort by.
4. In the page that appears, locate the field that you want to use to sort by, and then click the corresponding Sort check box.

![Field Sets](image)

Note: Review the Metadata Name column to identify the original metadata from which the field value is extracted.

5. Click Apply changes.

What’s Next?

- CES 7.0.6942–(August 2014) When you make an existing field a sort field, you must rebuild sources that are using a field set containing this field.
- CES 7.0.7022+ (September 2014) The index automatically processes the changes without a rebuild.
• Using the .NET Interface Editor, customize the search criteria available in the .NET search interface to help end-users sort results more conveniently (see "Adding Sort Criteria With the .NET Interface Editor" on page 624).

8.7.4.7.11 Managing Display Fields

A display field appears in search results of a .NET or JavaScript search interface (see "What Are Display Fields?" on page 620). Before you can add a display field to the search results from the .NET Interface Editor (see "Adding Display Fields to Search Results With the .NET Interface Editor" on page 620) or JavaScript Interface Editor (see JavaScript Search Interface Editor), the field must be set as a display field in the index. A display field is also visible in the Index Browser (see Reviewing Document Details from the Index Browser).

By default, all system and custom fields are set as display field in the index. You can change that when you create a field (see "Adding or Modifying Custom Fields" on page 494) or at anytime as described below. This is particularly useful when you import a field set in which one or more fields are not set as display fields and you want them to be.

To manage display fields

1. On the Coveo server, access the Administration Tool.
2. Select Configuration > Fields.
3. In the panel on the left, select the field set containing the display fields that you want to manage.
4. In the page that appears:
a. Select the **Display Field** check box for fields that you want to be able to add as a display field in a search interface or see in the index browser.

**Notes:**
- By default at query time, all display fields and their values are downloaded with search results. This is the only significant cost of display field. You may want to clear the **Display Field** check box for unused fields to minimize the search results download size.
- In the background this selection sets the **IncludeInResults** index property is set to **true**.

b. Click **Apply changes**.

**What's Next?**

Using the Interface Editor, add a display field to the result of a .NET search interface (see "Adding Display Fields to Search Results With the .NET Interface Editor" on page 620).

Trouble shoot field issues by inspecting their value in the index browser (see Reviewing Document Details from the Index Browser).

**8.7.4.8 Administration Tool - Field Aliases Menu**

A field alias set is a group of field aliases whose purpose is to establish mappings between existing fields and field names that are easier to remember and use in queries. Typically, a field alias eliminates the **sys** prefix.
Example: When the author field alias is defined for the sysauthor field, the query @author=Paul is automatically converted to @sysauthor=Paul by the field alias set.

The Coveo Platform comes with a default field alias set. You can create different field alias sets (see "Adding a Field Alias Set" on page 506), but you can only use one field alias set on an index at a time (see "Modifying or Using Advanced Index Parameters" on page 366). Within a field alias set, you can add, modify, or delete aliases (see "Managing Field Aliases" on page 506).

8.7.4.8.1 Adding a Field Alias Set

You can create field alias sets but only one field alias set is active on an index at a time (see "Administration Tool - Field Aliases Menu" on page 505).

Example: The default field aliases use English words. When most of your end-users are French speaking, you can create a field alias set with French aliases, and rather activate this field alias set on the index. Because you can only have one alias for a given field, you cannot create a multilingual field alias set.

To add a field alias set

1. On the Coveo server, access the Administration Tool.
2. Select Configuration > Field Aliases.
3. In the Add Field Alias Sets page, click Add.
4. In the Add Field Alias Set page:
   a. In the Name box, enter a name to identify the field alias set.
   b. In the Description box, enter a description of the field alias set.
   c. Click Save.

What's Next?

A newly created field alias set is a copy of the default field alias set. You must add, modify, or delete the field aliases it contains to customize it (see "Managing Field Aliases" on page 506).

8.7.4.8.2 Managing Field Aliases

Within a field alias set, you can add, modify, or delete field aliases (see "Administration Tool - Field Aliases Menu" on page 505).

You can only set one alias per field and an alias must be unique within an alias set. Consequently, when you want to change the alias associated with a field, you must first delete the alias, and then create a new one for this field.

Example: When you want to create a French alias for the sysauthor field, you must first delete the default author alias, and then add a new auteur alias for the sysauthor field.
8.7.4.8.2.1 Adding a new field alias

1. On the Coveo server, access the Administration Tool.
2. Select Configuration > Field Aliases.
3. In the Field Alias Sets page, click the field alias set to which you want to add a field alias.
4. In the Aliases page, click Add.
5. In the Add Field Alias page:
   a. In the Alias box, enter the name of the field alias. The alias must not contain spaces or accented and other special characters and is not case sensitive.
   
   Example: author
   
   b. In the Field box, enter the name of the corresponding field.
   
   Example: sysauthor.
   
   c. Click Save.

8.7.4.8.2.2 Modify an existing field alias

1. On the Coveo server, access the Administration Tool.
2. Select Configuration > Field Aliases.
3. In the Field Alias Sets page, click the field alias set that contains the field alias that you want to modify.
4. In the Aliases page, click the field alias that you want to modify.
5. In the corresponding page:
   a. In the Field box, modify the name of the field associated with this alias.
   
   b. Click Apply Changes.

8.7.4.8.2.3 Deleting an existing field alias

1. On the Coveo server, access the Administration Tool.
2. Select Configuration > Field Aliases.
3. In the Field Alias Sets page, click the field alias set that contains the field alias that you want to delete.
4. In the Aliases page:
   a. Select the check box of the field alias that you want to delete.
   
   b. At the top of the page, click Delete.
   
   c. At the deletion confirmation message, click Yes.
What's Next?

When you want the field alias changes to be effective on the index, ensure that the field alias set containing the added, modified, or deleted field alias is active on the index (see "Modifying or Using Advanced Index Parameters" on page 366).

8.7.4.9 Administration Tool - XML Menu

An XML document definition is a collection of XML elements which describe the structure of XML content found in a source in order to index it.

**Example:** A document definition can be created to index the content of a database sent to CES via an XML feed. In such cases, all document types found in the database must have a corresponding XML element (otherwise, they are not indexed).

8.7.4.9.1 Adding an XML Document Definition

An XML document definition is a collection of XML elements which describe the structure of XML content found in a source in order to index it. Because XML structures are variable, the Coveo Platform does not provide built-in XML document definitions. However, you can create different XML document definitions to reflect the structural specificities of each repository.

To add an XML document definition

1. On the Coveo server, access the Administration Tool.
2. Select Configuration > XML.
3. In the XML Document Definitions page, click Add.
4. In the Add XML Document Definition page:
   a. In the Name box, enter a name to identify the XML document definition.
   b. In the Description box, optionally enter a description of the XML document definition
      **Example:** Enter the list of repositories it is meant to index.
   c. Click Save.

8.7.4.9.2 Adding and Modifying XML Elements to a Document Definition

Each XML element details the content of a single XML document type (ex.: a thesaurus or bank of employee resumes). It lists the fields from which CES extracts information. Note that all document types found in a repository must have a corresponding element (otherwise, they are not indexed).

To add an XML element

1. On the Coveo server, access the Administration Tool.
2. Select Configuration > XML.
3. In the XML Document Definitions page, click the appropriate XML document definition.
4. In the **Record Definitions** page, click **Add**.

5. In the **Add a Record Definition** page:

   a. In the **Root XML Path** box, enter the path of the XML node corresponding to the document (in the form `RootElementNode/ElementNode`). Each root XML path must be unique within an XML document definition.

   b. **Under Properties**, enter XML relative paths in the form `%[xmlNodePath@attributeName]` to build the value for each property.

For a description of the property fields, refer to the table below.

<table>
<thead>
<tr>
<th>Property</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Title</strong></td>
<td>Identifies the title of the document.  &lt;br&gt;<strong>Example:</strong> If <code>%[@Title]</code> is entered, CES searches for an XML node attribute entitled <em>Title</em> from which to extract the information.</td>
</tr>
<tr>
<td><strong>Author</strong></td>
<td>Identifies the author of the document.  &lt;br&gt;<strong>Example:</strong> If <code>%[@Author]</code> is entered, CES searches for an XML node attribute entitled <em>Author</em> from which to extract the information.</td>
</tr>
<tr>
<td><strong>Content</strong></td>
<td>Identifies the content of the document.  &lt;br&gt;<strong>Example:</strong> If <code>%[@Description]</code> is entered, CES searches for an XML node attribute entitled <em>Description</em> from which to extract the information.</td>
</tr>
<tr>
<td><strong>Summary</strong></td>
<td>Identifies the summary of the document.  &lt;br&gt;<strong>Example:</strong> If <code>%[@Summary]</code> is entered, CES searches for an XML node attribute entitled <em>Summary</em> from which to extract the information. If this field is left empty a summary is automatically extracted by CES.</td>
</tr>
<tr>
<td><strong>Date</strong></td>
<td>Identifies the date of the document (creation or modification date).  &lt;br&gt;<strong>Example:</strong> If <code>%[@CreationDate]</code> is entered, CES searches for an XML node attribute entitled <em>CreationDate</em> from which to extract the information. If those fields are left empty, the parent XML document date is issued.</td>
</tr>
<tr>
<td><strong>Address</strong></td>
<td>Identifies the link to open when a search result is clicked.  &lt;br&gt;<strong>Example:</strong> If <code>%[@URI]</code> is entered, CES searches for an XML node attribute entitled <em>URI</em> from which to extract the information. When a user clicks the search result, the value of the metadata is used to open the document. If this field is left empty, the parent XML document is opened when the search result is clicked.</td>
</tr>
<tr>
<td>Property</td>
<td>Definition</td>
</tr>
<tr>
<td>-------------</td>
<td>------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Unique ID</td>
<td>Only identifies the record within the XML document. This information is used to construct the URL of the document and is useful to locate a particular record on big XML documents. If this field is left empty, a sequential number is used as the unique ID. Example: If <code>%[0ID]</code> is entered, CES searches for an XML node attribute entitled ID from which to extract the information.</td>
</tr>
</tbody>
</table>

c. In the **Date Format** box, enter the format of the dates contained in the XML document (see "Specifying a Date Format" on page 499).

d. Click **Save**.
Example: The following XML document regroups employee resumes. Its root element is `Department` and its record node is `Employee`; therefore, its root XML path is `Department/Employee`.

```xml
<?xml version="1.0" ?>
<Department>
  <Employee ID="123" URI="http://svr-db/companyinfo/employees?ID=123">
    <CreatedBy>Mary Smith</CreatedBy>
    <Name>
      <First>Jack</First>
      <Last>Jackson</Last>
    </Name>
    <Address Street="123, Main Avenue" City="Cityville" Zip="12345"/>
    <HiringDate>2004/02/01 00:00:00</HiringDate>
    <Resume>A dynamic administrator with a strong record of achievement combining skills in diverse areas of organizational development, group/staff leadership, program development and project management, building partnerships and community relations. Experienced in the operation of a successful consulting practice, the turn around of a second small business, and the administration of several non-profit organizations. Highly motivated and intuitive, effective at human relations, and able to manage both time and resources to maximize productivity</Resume>
  </Employee>
  <Employee ID="456">
    <CreatedBy>Mary Smith</CreatedBy>
    <Name>
      <First>John</First>
      <Last>Johnson</Last>
    </Name>
    <Address Street="123, Generic Street" City="Urbanville" Zip="12345"/>
    <HiringDate>2003/02/07 00:00:00</HiringDate>
    <Resume>Twelve years successful experience in direct sales of a range of products and services. Extensive practical hands-on experience as co-owner and manager of a small business. Motivated and enthusiastic about developing good relations with clients. Effective working alone or as a cooperative team member. Professional in appearance and presentation.</Resume>
  </Employee>
</Department>
```

The XML element corresponding to this document is:
What's Next?

Rebuild the source (see "Applying an Action to a Collection or a Source" on page 283).

8.7.4.9.3 Associating an XML Document Definition to a Source

An XML document definition is a collection of XML elements which describe the structure of XML content found in a source in order to index it. Because XML structures are variable, the Coveo Platform does not provide built-in XML document definitions. However, you can create different XML document definitions to reflect the structural specificities of each repository (see "Adding an XML Document Definition" on page 508 and "Adding and Modifying XML Elements to a Document Definition" on page 508).

Once an XML document definition is configured you can assign it to one or more sources.

To associate an XML document definition to a source

1. On the Coveo server, access the Administration Tool.
2. Select **Index > Sources and Collections**.
3. In the **Sources and Collections** page:
a. In the Collections section, select the collection containing the source that you want to modify.

b. In the Sources section, expand the appropriate source drop-down list, and then select Edit XML Document Definition.

4. In the XML Document Definition page corresponding to the source:

a. In the XML Document Definition drop-down list, select the appropriate XML document definition.

b. Click Apply Changes.

8.7.4.10 Administration Tool - SharePoint Menu

This section regroups topics that help you to configure CES to index the Windows SharePoint Services (WSS) and SharePoint Portal Server (SPS whose 2007 version is called MOSS) using the provided structures described in the SharePoint references sets (see "Adding a SharePoint Reference Set" on page 514).

8.7.4.10.1 What Is the Structure of SharePoint?

SharePoint is a server-based application designed to regroup and organize information. SharePoint is composed of two products: Windows SharePoint Services (WSS) and SharePoint Portal Server (SPS whose 2007 version is called MOSS). WSS is a free add-on to Windows Server and offers basic intranet functionalities (creation of team sites and project sub-sites, etc.); whereas, SPS is a more advanced service, built on WSS, which offers complete classification and collaboration capabilities. WSS, SPS and MOSS can be indexed by the Coveo Platform using the provided structures described in the SharePoint references sets (Configuration > SharePoint).

SharePoint contains Web-like and database-like features called items. The following table summarizes the properties or these features into item types which are indexed differently.

<table>
<thead>
<tr>
<th>Item type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Portal</td>
<td>Identifies the root of SPS. Portals provide unified access to all other content (areas, lists, etc.).</td>
</tr>
<tr>
<td>Area</td>
<td>Identifies sub-sites of the portal. Areas regroup entries on a specific subject (ex.: news).</td>
</tr>
<tr>
<td>AreaListing</td>
<td>Identifies entries of an area. Area listings are frequently used to link to other content inside or outside the portal.</td>
</tr>
<tr>
<td>Site</td>
<td>Identifies the root of WSS. If SPS is used, sites are accessible through the portal.</td>
</tr>
<tr>
<td>SiteItem</td>
<td>Identifies binary (i.e. unstructured) documents contained in a site (ex.: .pdf or .docx documents).</td>
</tr>
</tbody>
</table>

Example: A specific news article constitutes an area listing of the News area.

Note: Sites created by users to present themselves and their tasks are called personal sites.
**8.7.4.10.2 What Are SharePoint Reference Sets?**

A reference set is a group of references (i.e. elements detailing the structure of a single SharePoint item) which describes the architecture of a SharePoint environment and, therefore, allows the Coveo Platform to index its content.

The **Default** reference set included with CES contains a reference for each SharePoint 2007 and 2010 built-in templates (ex: Announcements, Contacts, etc). However, new references must be added for each custom template used and, if an existing template is modified, its corresponding reference must be updated as well; otherwise, erroneous or blank results are returned by queries (ex.: the content and summary can be inverted and the author name missing). It is also possible to create different reference sets to reflect the structural specificities of each SharePoint repository.

**Note:** SharePoint references are used only to index structured information; unstructured information is automatically extracted using the corresponding converter or IFilter.

**8.7.4.10.3 Adding a SharePoint Reference Set**

A reference set is a group of references (i.e. elements detailing the structure of a single SharePoint item) which describes the architecture of a SharePoint environment and, therefore, allows CES to index its content. You can create different reference sets to reflect the structural specificities of each SharePoint repository.

To add a reference set:

1. On the Coveo server, access the Administration Tool.
2. Select **Configuration > SharePoint**.
3. In the **SharePoint Reference Sets** page, click **Add**.
4. In the **Add SharePoint Reference Set** page:
a. In the **Name** box, enter a name to identify the reference set.

b. In the **Description** box, optionally enter a description of the reference set.

**Example:** Enter a list of the SharePoint repositories it is meant to index.

c. Click **Save**.

**What's Next?**

The reference set created is identical to the default one. You must add new or modify existing references for each custom template used (see "Adding and Modifying SharePoint References" on page 515).

When an existing template is modified, its corresponding reference must be updated as well; otherwise, erroneous or blank results are returned by queries (ex.: the content and summary can be blank and the author name missing).

**8.7.4.10.4 Adding and Modifying SharePoint References**

Each reference details the structure of a single SharePoint item (portal, area, site, etc.). The reference lists the fields from which CES must extract information. New references must be added for each custom template used and, if an existing template is modified, its corresponding reference must be updated as well; otherwise, erroneous or blank results are returned by queries (ex.: the content and summary can be blank and the author name missing).

**Note:** SharePoint references are used only to index structured information. Unstructured information is automatically extracted using the corresponding converter or IFilter.

**To add a reference**

1. On the Coveo server, access the Administration Tool.

2. Select **Configuration > SharePoint**.

3. In the **SharePoint Reference Sets** page, click the reference set to which you want to add a reference.

4. In the **References** page, click **Add**.

5. In the **Add a SharePoint Reference** page:

   a. In the **Item Type** drop-down list, select the type of the item (see "What Is the Structure of SharePoint?" on page 513).

   b. If the item type is **List** or **List Item** and the reference applies to all items (ex.: all **Agenda** lists), select the appropriate list type in the **List type** drop-down list.

   c. If the reference applies to a specific item (ex.: a single portal or site), select **Specific portal/area/site** or **List name** and enter the item name (ex.: **CoveoPortal**).

   d. In the **Properties** section, enter the metadata tags corresponding to the appropriate SharePoint columns (in the form %[metadataname]).

      For more information, refer to the table below.
<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
</table>
| Title    | Identifies the title of an item.  
**Example:** If `%%[Title]` is entered, CES searches for a SharePoint metadata tag named *Title* from which to extract the information. |
| Author   | Identifies the author of an item.  
**Example:** If `%%[Author]` is entered, CES searches for a SharePoint metadata tag named *Author* from which to extract the information. |
| Content  | Identifies the content of an item.  
**Example:** If `%%[Description]` is entered, CES searches for a SharePoint metadata tag named *Description* from which to extract the information. |
| Summary  | Identifies the summary of an item.  
**Example:** If `%%[Summary]` is entered, CES searches for a SharePoint metadata tag named *Summary* from which to extract the information.  
**Note:** If this field is left blank, a summary is created from the content of the document. |
| Date     | Identifies the modification date of an item.  
**Example:** If `%%[Modified]` is entered, CES searches for a SharePoint metadata tag named *Modified* from which to extract the information. |
| Address  | Identifies the link to open when a search result is clicked.  
**Example:** If `%%[customUrl]` is entered, CES searches for a SharePoint metadata tag named *customUrl* from which to extract the information. When a user clicks on the search result of this SharePoint type, the value of the metadata is used to open the document. If nothing is entered, the normal item URL is used to open the document. |

Note: If this field is left blank, a summary is created from the content of the document.

### e. In the **Date Format** box, enter the format of the dates contained in the item (see "Specifying a Date Format" on page 499).

**Note:** If the Date Format box is left blank, CES automatically associates the dates encountered with one of the formats in its memory. However, if the format used is not in the CES memory, dates are not indexed.

### f. Click **Apply Changes**.

To modify a reference

1. On the Coveo server, access the Administration Tool.
2. Select **Configuration > SharePoint**.
3. In the **SharePoint Reference Sets** page, click the reference set in which you want to modify a reference.
4. In the **References** page, click the reference that you want to modify.
5. In the page for the selected reference:
a. In the **Properties** section, modify the appropriate tags. For more information, refer to the table in the previous procedure.

**Important:** Property values are built by replacing each `%[metadata]` tag by the metadata value; therefore, it is possible to create a property value using several metadata. Note that if a metadata is not found in the indexed document, the metadata tag is removed from the property value.

**Example:** If a document has these two metadata:

<table>
<thead>
<tr>
<th>Name</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>UserFirstName</td>
<td>John</td>
</tr>
<tr>
<td>UserLastName</td>
<td>Smith</td>
</tr>
</tbody>
</table>

The following table displays the property values for each property entered:

<table>
<thead>
<tr>
<th>Entered value</th>
<th>Generated value</th>
</tr>
</thead>
<tbody>
<tr>
<td>%[UserLastName]</td>
<td>Smith</td>
</tr>
<tr>
<td>%[UserLastName], %[UserFirstName]</td>
<td>Smith, John</td>
</tr>
<tr>
<td>%[UserFirstName], last name is %[UserLastName]</td>
<td>John, last name is Smith</td>
</tr>
<tr>
<td>%[UserFirstName] %[BadMetadata]</td>
<td>John</td>
</tr>
</tbody>
</table>

**Note:** New properties can be added in order to index additional data (see "Adding New Properties to SharePoint References" on page 519).

b. Click **Apply Changes**.

8.7.4.10.5 How CES Indexes SharePoint Items

When the Coveo Platform indexes a SharePoint source, it associates each item with its corresponding reference—the tags contained in the reference are subsequently used to extract content and metadata. Therefore, it is crucial that each reference reflects the structure of its SharePoint item—new references must be added for each custom template used and, if an existing template is modified, its corresponding reference must be updated as well; otherwise, erroneous or blank results are returned by queries (ex.: the content and summary can be blank and the author name missing).

Moreover, if CES is unable to associate a reference with an item, it takes one of two actions: for lists and list items, it uses the **List - Unknown** or **List Item - Unknown** reference; whereas, for other items, it indexes file information only (i.e. index by reference).

The following diagram outlines the process performed by CES to associate a SharePoint item with its corresponding reference:
8.7.4.10.6 Available Item Types

Every indexed item or document of a SharePoint source has an item type that you can find using the @sysspitemtype query.

The following table lists the possible item types.

<table>
<thead>
<tr>
<th>Item types</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Area</td>
<td>Represents a SharePoint area (SPS 2003 only)</td>
</tr>
<tr>
<td>AreaListing</td>
<td>Represents a SharePoint area listing (SPS 2003 only)</td>
</tr>
<tr>
<td>List</td>
<td>Represents a SharePoint list</td>
</tr>
</tbody>
</table>
### Item types Description

<table>
<thead>
<tr>
<th>Item types</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ListItem</td>
<td>Represents an item of a SharePoint list or document of a SharePoint document library</td>
</tr>
<tr>
<td>ListItemAttachment</td>
<td>Represents an attached document on a SharePoint list item</td>
</tr>
<tr>
<td>Portal</td>
<td>Represents a SharePoint portal root site (SPS 2003 and MOSS 2007 only)</td>
</tr>
<tr>
<td>Site</td>
<td>Represents a SharePoint site</td>
</tr>
<tr>
<td>SiteItem</td>
<td>Represents a document in a SharePoint site that is not in a document library</td>
</tr>
<tr>
<td>UserProfile</td>
<td>Represents a SharePoint user profile (SPS 2003 and MOSS 2007 only)</td>
</tr>
</tbody>
</table>

8.7.4.10.7 Available List Base Types

The `@sysplistbasetype` field contains the list base type.

The five base types for a SharePoint list are:

- Custom
- DiscussionBoard
- DocumentLibrary
- Issues
- Survey

**Note:** For more information, refer to the following Microsoft document: `BaseUrl Element`

8.7.4.10.8 Adding New Properties to SharePoint References

Each reference details the structure of a single SharePoint item (portal, area, site, etc.)—it lists the fields from which CES must extract information. New references must be added for each custom template used and, if an existing template is modified, its corresponding reference must be updated as well; otherwise, erroneous or blank results are returned by queries (ex.: the content and summary can be blank and the author name missing).

In order to index additional information (ex.: language) a custom field must be created in the Custom Fields page—each custom field is displayed in the reference page below the Properties section.

**Note:** SharePoint references are used only to index structured information. Unstructured information is automatically extracted using the corresponding converter or IFilter.

To create a custom field for SharePoint references

1. On the Coveo server, access the Administration Tool.
2. Select Configuration > Fields.
3. In the Field Sets page, click a field set.
4. In the **Custom Fields** page, click **Add**.

5. In the **Add a Custom Field** page:

   ![Custom Field Configuration](image)

   a. In the **Name** box, enter a name to identify the field.

   b. In the **Type** section, select the appropriate field type (see "Adding or Modifying Custom Fields" on page 494).

   c. In the **Metadata Name** box, enter any non-empty value (the actual metadata name is entered in the reference page in the form %[metadataname]).

   d. In the **Default Value** box, enter the field type (ex.: string). The default value is indexed when a field is empty.

   ![Note](image)

   **Note:** If the field applies only to SharePoint items, the **Options** and **Date format** sections (displayed when **Date/time** is selected in the **Type** section) are not important because all the pertinent information is provided when the reference is added (see "Adding and Modifying SharePoint References" on page 515). However, if the custom field is used to index binary (unstructured) documents as well, refer to the procedure provided in "Adding or Modifying Custom Fields" on page 494.

   e. Click **Save**.

The custom fields from all sets appear in the in the SharePoint reference page.
8.7.4.10.9 What Is the Difference between Structured and Unstructured Information?

The term *structured information* describes the data contained in fields. It is called *structured* because its nature and function are identified by metadata tags. All content created directly within SharePoint (ex.: list items and area listings) is structured. Whereas, the term *unstructured information* describes binary documents (ex.: .pdf and .docx documents) added using proprietary applications such as Acrobat or Word. SharePoint references are used only to index structured information; unstructured information is automatically extracted using the corresponding converter or IFilter.

8.7.4.10.10 Indexing Structured Information in SharePoint Sources

The term *structured information* describes data contained in fields because its nature and function are identified by metadata tags—all content created directly within SharePoint (ex.: list items and area listings) is structured.

Two elements are required in order to index the structured information contained in SharePoint: a SharePoint or custom field to indicate how CES should sort the information and a reference to indicate where CES should search for the information. SharePoint fields are built into CES. You can create a custom field to index structured information not extracted by SharePoint fields (see "Adding New Properties to SharePoint References" on page [link])
Finally, you can create a new reference or modify an existing one (see "Adding and Modifying SharePoint References" on page 515).

8.7.4.10.11 Determining the Name of a SharePoint Metadata Tag

In SharePoint, structured information like list items and area listings is identified by metadata tags which describe its nature and function. CES uses these tags to sort the information.

**Note:** If the tags entered do not correspond to the metadata names of the appropriate SharePoint fields, erroneous or blank results are returned by queries (ex.: the content and summary can be blank and the author name missing).

To determine the metadata name of a column

1. In SharePoint, access the page where the list is displayed.
2. Click the column name for which you want to determine the metadata name.
3. In the Address box of the browser, locate the expression `SortField=`. The name of the column is the expression entered after `=`, in the `SortField=Name` form.

**Example:** In the following capture, the metadata name for the **Name** column is **LinkFilename**.

8.7.4.10.12 Indexing Unstructured Information in SharePoint Sources

The term *unstructured information* describes binary documents (ex.: .pdf and .docx documents) added using proprietary applications such as Acrobat or Word—it is automatically extracted using the corresponding converter or IFilter. However, its metadata is not indexed using SharePoint references (as for structured information)—it must be extracted using built-in or custom fields.

8.7.4.11 Administration Tool - License Menu

You can access the **License** page to retrieve information concerning your current Coveo Enterprise Search (CES) license. You can also upgrade or enter a new license code.
8.7.4.11.1 About the Coveo License

The Coveo Master server requires Coveo license information to operate (see "What Information Is Displayed in the License Page?" on page 525).

Coveo sends an email message entitled Coveo Enterprise Search License Information to the email address that was entered in the registration form for your organization. The message contains a Coveo Enterprise Search License Code.txt file attachment as well as links to download the CES installer.

After installing CES on the Master server, when you create a new index or convert an existing one, an empty Enter License Code page of the Administration Tool automatically appears where you must paste the Coveo license information (see "Entering a New License Code" on page 523).

8.7.4.11.2 Entering a New License Code

You receive your Coveo license as a text file (Coveo Enterprise Search License.txt) attached to an email sent to you from Coveo. This file contains a description of the CES version for which the license is intended, as well as the encrypted licensing information.

You need to copy the encrypted licensing information into the Enter License Code page of the Coveo Administration Tool to activate the license.

You can update CES with a valid license code at anytime without any service downtime.
Notes:

- The Notes: The Enter License Code page automatically appears at the end of the CES installation. page automatically appears at the end of the CES installation.

- You get the following error message when you attempt to use a Coveo for Sitecore license in the CES Enter License Code page:

```
The license is invalid.
The entered license appears to be one for Coveo for Sitecore. If you purchased a Coveo Enterprise Search license, enter it below. For the Coveo for Sitecore Free Edition, close this page. Start the Coveo for Sitecore installation where you will be prompted for your Coveo for Sitecore license.
```

You must rather provide this type of license in the Coveo for Sitecore license wizard (see Updating the Coveo for Sitecore License).

To enter a new license code

1. Open the Coveo Enterprise Search License email that you received from Coveo.

2. Using a text editor such as Notepad:
   a. Open the Coveo Enterprise Search License.txt attachment file.
   b. Select the license code, ensuring that you include the `{BEGIN LICENSE}` and `{END LICENSE}` tags.
   c. Right-click the selection, and then select Copy.

3. If the Enter the License Code page has not been opened by the CES installer:
a. On the Coveo server, access the Administration Tool.

b. In the Administration Tool, select Configuration > License.

c. In the License page, click Enter New License Code.

Note: The Enter New License Code link is disabled (grayed out) when the index is in read-only mode, because the license cannot be changed in this mode. You must switch the index back to the read-write mode to enable the link (see "Toggling the Index Between the Read-Write and Read-Only Modes" on page 263).

4. In the Enter License Code page of the Administration Tool:

a. In the License box, right-click and select Paste to paste the license code from the license file.

b. Click Apply Changes.

The Administrator Tool Configuration > License page appears. Your Coveo Master server is ready to operate.

What's Next?

When you enter the license following the installation of CES on the Master server, continue the deployment process by installing the Coveo Front-End components (see "Installing Coveo .NET Front-End" on page 43 and "Coveo Platform Deployment Overview" on page 12).

8.7.4.11.3 What Information Is Displayed in the License Page?

The License page displays information concerning the license used by the Coveo server and allows to upgrade it. Referring to this page is useful to validate restrictions associated with your current Coveo license.
## License Information

<table>
<thead>
<tr>
<th>Allowed Sources</th>
<th>Denied Sources</th>
<th>Expiration</th>
<th>Query Expiration</th>
<th>Support Plan Expiration</th>
<th>Available Search Interfaces</th>
<th>Document Restrictions</th>
<th>Allowed OCR Converters</th>
<th>Audio Video Restrictions</th>
<th>Configuration Restrictions</th>
<th>Feature Restrictions</th>
<th>Super Users Allowed</th>
<th>Analytics Allowed</th>
<th>Computed Facets Allowed</th>
<th>Text Analytics Allowed</th>
</tr>
</thead>
<tbody>
<tr>
<td>Active Directory</td>
<td>None</td>
<td>None</td>
<td>Will expire on 4/10/2016</td>
<td>Will expire on 4/10/2016</td>
<td>SharePoint Search Interface</td>
<td>None</td>
<td>2</td>
<td>Maximum of 1 audio video converter</td>
<td>None</td>
<td>None</td>
<td>None</td>
<td>None</td>
<td>None</td>
<td></td>
</tr>
<tr>
<td>Confluence</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Default Search Interface</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Database</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Desktop Connector</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Discourse</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Documentum</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Dropbox</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Bitnami CMS</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Exchange (WebDav)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Exchange (WebServices)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Exchange2</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Files</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Google Drive (Google Apps)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Google Drive (Single User)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Google Sites</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Jira v2</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Jive</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Jive 5 / SBS / Clearspace</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>LDAP</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Litaiy</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Lithium</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Microsoft Dynamics CRM</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Notes</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>OpenText Content Server / Lifelink</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Oracle UCM</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Queue</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Review Board</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>RSS</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Salesforce</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Salesforce (Legacy)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Script</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SharePoint</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SharePoint (Legacy)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Sitecore</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Sitecore (Legacy)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Sybase Enterprise Vault</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>TargetProcess</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Twitter</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Web</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>WebScraper</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>WebSphere WCM</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Windchill</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Yammer</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
The following table describes the information available in the **License** page.

<table>
<thead>
<tr>
<th>Section</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>License</strong></td>
<td>Indicates the name of the person or organization to which the license was delivered.</td>
</tr>
<tr>
<td><strong>Allowed Sources</strong></td>
<td>Lists the connectors available with this license.</td>
</tr>
<tr>
<td><strong>Denied Sources</strong></td>
<td>Lists the connectors not available with this license.</td>
</tr>
<tr>
<td><strong>Expiration</strong></td>
<td>Indicates the date on which the license must be renewed. Evaluation licenses are valid for 30 days. Full licenses either expire at a specific date or are perpetual as stated in the user contract.</td>
</tr>
<tr>
<td><strong>Query Expiration</strong></td>
<td>Indicates the date on which the search queries will no longer be processed.</td>
</tr>
<tr>
<td><strong>Support Plan Expiration</strong></td>
<td>Indicates the date on which the premium support plan must be renewed. Premium support is valid for a year (unless stated otherwise in the support contract).</td>
</tr>
<tr>
<td><strong>Available search interfaces</strong></td>
<td>Indicates whether the SharePoint search interface is available in addition to the default search interface.</td>
</tr>
<tr>
<td><strong>Document Restrictions</strong></td>
<td>Indicates the total number of documents it is possible to index with this license.</td>
</tr>
<tr>
<td><strong>Notes:</strong></td>
<td>To index additional documents, the license must be upgraded.</td>
</tr>
<tr>
<td></td>
<td>You receive notifications when the index is close or reaching the document number limit (see &quot;License Document Limit Notifications&quot; on page 528).</td>
</tr>
<tr>
<td><strong>Allowed OCR Converters</strong></td>
<td>CES 7.0.6684+ (May 2014) indicates the maximum number of optical character recognition converters which can be used concurrently with the OCR Module (see &quot;OCR Module&quot; on page 678).</td>
</tr>
<tr>
<td><strong>Configuration Restrictions</strong></td>
<td>Indicates whether the number of mirrors is limited with this license. The main index on the Coveo Master server is technically a mirror. The value A single mirror by physical index means that the license allows only the Master server. When you want to install one Mirror server, you must have a license allowing two mirrors.</td>
</tr>
<tr>
<td><strong>Feature Restrictions</strong></td>
<td>Indicates whether some features are disabled with this license.</td>
</tr>
<tr>
<td><strong>Super Users Allowed</strong></td>
<td>Indicates if the super user access is available.</td>
</tr>
<tr>
<td><strong>Analytics Allowed</strong></td>
<td>Indicates if the Usage Analytics Module is available (see &quot;On-Premises Usage Analytics Module&quot; on page 649).</td>
</tr>
</tbody>
</table>
### 8.7.4.11.4 License Document Limit Notifications

Your Coveo license can come with restrictions such as a limited number of documents that can be indexed by CES. In such cases, CES sends an email notification when you are about to reach the limit and another one when you reach it. CES administrators can decide who receive these emails in the **Alerts** page of the Admin Tool (see Configuring Email Alerts).

The first message is sent when 80% of the document limit is reached and looks like the following:

**Example:** You are using 800000 of your 1000000 document limit. To upgrade your license, visit our Web site at [www.coveo.com/go/?dest=license-expiration](http://www.coveo.com/go/?dest=license-expiration)

The second message is sent when the document limit is reached and looks like the following:

**Example:** The program has reached the maximum number of 1000000 documents allowed. Cannot add any more 52 documents.

**Note:** At all time, you can monitor the number of documents in your index versus your document restrictions (see [Administration Tool - Overview Menu](#) and [What Information Is Displayed in the License Page?](#)).

### 8.7.4.12 Administration Tool - Alerts Menu

This section contains a topic showing how to configure CES to send email alerts whenever a CES error or important issues occur and you need to quickly react without having to regularly refer to the CES console and logs to monitor the system.

#### 8.7.4.12.1 Configuring Email Alerts

You can configure CES to send email alerts whenever a CES error occurs. This feature is useful to allow you to quickly react when important CES issues occur without having to regularly refer to the CES console and logs to monitor the system. You can set the alerts to be sent for any type of CES errors or only for fatal CES errors.

A fatal CES error is an unhandled exception that stops the CES service and generates a core dump of the CES process state. As the CES process typically occupies several gigabytes of memory, the core dump to the hard disk can take a few minutes during which the CES service is interrupted. As the CES service is normally set to restart automatically, the CES service will become available again within minutes.

**Examples:** Fatal errors can be caused by insufficient hard disk space, hardware errors preventing reading/writing to the hard disk, insufficient memory.

Fatal CES errors will not occur when the Coveo instance is properly configured and has access to sufficient computer resources. It is recommended to configure the email alerts for fatal CES errors.
Example: The content of a CES email alert for a fatal error:

```
#Version: 6.5 build 4721
#Server: svr-ces03 (coveo\svc_cesservice)
#Instance: CES
#Date: 2012/01/30 16:24:02
#Severity: FATAL

Unhandled exception in Default-TrnManager - Alloc: Failed to allocate: 128 bytes. Used 3728660 k (peak:5131584k).
```

Non fatal CES errors are significantly more frequent as they can be the consequence of a large number of causes. In real life several non fatal CES errors can occur daily. Configuring the email alert for non fatal errors can generate a significant number of email messages.

Examples: Non fatal CES errors can be:

- For the index: document conversion error, script error, insufficient hard disk space for the compaction.
- For connectors: timeout or loss of connection with the repository, corrupted database, invalid XML returned, too many retries.

Note: Errors occurring in Coveo Front-End processes are not logged in the CES log and therefore do not appear in email alerts.

To configure email alerts:

1. On the Coveo server, access the Administration Tool.
2. Select Configuration > Alerts.
3. In the Alerts page:
In the Alert when drop-down list, select one of the following options:

**Never**

Disables the email alerts.

**An Error Occurs**

Sends an email each time a fatal or non fatal CES error occurs.

**A Fatal Error Occurs**

Sends an email each time a fatal CES error occurs.

b. Beside Email Settings:

i. In the Sender address box, enter the email address used by CES to send the alerts.

ii. In the Recipient addresses box, enter one or more semicolon separated Coveo administrator email addresses to which CES sends the alerts.

iii. In the Subject box, enter text used for the email subject.

c. Beside SMTP Server, configure the SMTP mail server to which CES has access to send the email alerts:

i. In the Server Address box, enter the address of your SMTP mail server.

ii. In the Port box, change the SMTP port number when it is different from the default value (25).

iii. When your SMTP server requires authentication, in the Username and Password boxes, enter the
credentials of a valid SMTP mail server.

iv.  **CES 7.0.7338+ (January 2015)** When you use an SMTPS mail server, select the **Use SSL connection** check box.

d.  Click **Send Test Email** to validate your email alert configuration. Verify that a CES email alert message was received by the recipients.

   If the test email is not sent to recipients within a few minutes, modify the configuration, and then Click **Send Test Email** again.

e.  Click **Apply Changes**.

8.7.4.13 Administration Tool - Pre-loading Menu

Use this menu to configure CES to keep the Coveo .NET search page applications continuously loaded in IIS and prevent a significant delay to display a search page when the application has to be reloaded (see "Why does the Initial .NET Search Page Take Much Longer to Appear?" on page 145).

8.7.4.13.1 Pre-Loading a .NET Search Page to Prevent Display Delays

You can configure CES to continuously send wake up requests to a .NET search application. The purpose of this configuration is to keep the Coveo .NET search application alive in IIS and prevent a significant delay to display a .NET search page when the application has to be reloaded (see "Why does the Initial .NET Search Page Take Much Longer to Appear?" on page 145).

When you perform the first-time setup of a Coveo .NET Front-End search interface, this search page is automatically registered to be warmed up in the **Pre-loading** page of the Administration Tool (see "Coveo .NET Front-End First Time Setup" on page 47). You may still need to manually add a .NET search interface for pre-loading in some cases.

**Examples:**

- When you use a Coveo JavaScript Search interface, the pre-loading configuration must be done manually.

- When your Coveo .NET Front-End servers are accessed through a network load balancer (NLB), the first time setup adds the NLB URL. You need to manually add the URL of each front-end server.

The configuration schedules the CES service to send an HTTP GET request with a wake up query argument (&wakeup=1) to the search page URL every 60 seconds. The request warms up all skins of the /Web/Coveo/Skins folder on the Coveo Front-End server.

When your Coveo configuration includes more than one Front-End server in an NLB cluster or not, repeat the following procedure to enter the URL of each server, not the address of a NLB cluster. Similarly, when a Front-End server has more than one application serving search pages, repeat this procedure to enter the URL of each application.
Notes:

- When you get error messages like the following:

  An error occurred while warming up search page [URL]: class CGLNetwork::NetworkAccessDenied: The login information of server (SERVER NAME) is invalid.

  follow the procedure in this topic and ensure that you properly configure the Address and the Authentication parameters, or when the search page no longer exists, delete its address (see "Removing a Pre-Loaded Search Page" on page 533).

- The search page warm up feature also triggers the tagging refresh processes that are often used in customer service solutions. Tags are fields that are populated with information gathered by post-indexing processes.

  When your customer solution takes advantage of tagging, you must set one search page to be warmed up to ensure that the tags remain up-to-date.

  When your Coveo instance includes more than one Front-End server, avoid warming up search pages from several servers as they will trigger duplicate tagging refresh processes that can waste Master server resources.

To pre-load a search page to prevent initial display delays

1. On the Coveo server, access the Administration Tool.
2. Click the Configuration tab, and then click the Pre-loading menu.
3. In the Pre-loading page, click Add.
4. In the Edit Search Page page:
   a. In the Name box, enter a name describing the search page that you want to automatically warm up.

      This name only appears in the Pre-loading page.
b. In the **Address** box, enter the URL of one search that you want to automatically warm up. Ensure to enter a URL that the Back-End server can resolve.

**Examples:**

- Enter the URL of your default Coveo web search page:
  

- Enter the URL of a search page on a SharePoint server:
  
  https://intranet.mycompany.com/CoveoSearch.aspx

- When Coveo .NET Front-End and Coveo Enterprise Search are installed on different servers, do not use http://localhost:8080, because the page is not available from the Back-End server.

c. When the search page cannot be accessed anonymously, in **Authentication**, select a user identity that has access to the search page.

**Note:** If the password of this account changes, you must update the password in the user identity to prevent warm up errors.

You can modify an existing user identity or create a new one respectively by clicking **Edit** or **Add** (see "Adding a User Identity" on page 420).

d. Click **Test Search Page** to validate the connection to the search page.

When the connection cannot be established, modify your settings and test again.

e. When the connection is successful, click **Apply Changes**.

### Removing a Pre-Loaded Search Page

1. On the Coveo server, access the Administration Tool.
2. Click the **Configuration** tab, and then click the **Pre-loading** menu.
3. In the **Pre-loading** page, under **Pre-loading**, select the check box of the search page for which you want to stop the warm up, and then click **Delete**.

**Note:** When your customer solution takes advantage of tagging, ensure to leave one search page to be warmed up so that the tags remain up-to-date.

### 8.7.4.14 Administration Tool - Advanced Menu

The **Advanced** menu allows you to fine-tune the performance of the Coveo Platform by modifying advanced configuration parameters.

#### 8.7.4.14.1 Modifying Advanced CES Parameters

You can fine-tune the performance of the Coveo Platform by modifying advanced configuration parameters.
To modify the advanced configuration parameters

1. On the Coveo server, access the Administration Tool.
2. Select Configuration > Advanced.
3. In the Advanced page:

   a. Next to Performance, configure the priority of CES processes. Five levels of priority exist (Highest, Above Normal, Normal, Below Normal and Lowest). Processes with highest priority are handled first, while processes with lowest priority are handled last. Processes with the same priority are handled in chronological order.

      Example: You can temporarily increase the indexing and crawling thread priorities when you index or rebuild a large repository during off-peak hours.

Main process priority
   Determines the priority of all CES processes in relation to other processes running on the server.

Indexing thread priority
   Determines the priority of the indexing process (i.e. converting and committing transactions) in relation to other CES processes such as querying.

Crawling thread priority
   Determines the priority of the crawling process (i.e. downloading information from repositories) in relation to other CES processes such as querying.
Number of query threads

Determines the number of threads assigned to the processing of queries.

b. In Port, you can change the port used to communicate with the CES service (see "About the CES Service Port" on page 230). Change this value only when you cannot use the default value (52800). When you change the port value here, you must also change the CES service port in Front-End servers of this Coveo instance (see "Changing the CES Service Port" on page 348).

Example: When you plan to upgrade the Coveo Platform from one major version to another, like from version 6.x to 7.x, you can install the two instances on the same Master server, but you need to ensure that the two instances use different CES service port numbers, like 52800 for version 6.x and 52801 for version 7.x.

c. In Maximum Terms per Query, you can change the maximum number of terms (excluding operators) that the index accepts for a query. The default is 128.

While it is unlikely that end-users type so many keywords in one query, programmed queries built from contextual information may include a large number of terms.

When a query exceeds the maximum number of terms, the extra terms are ignored, the query is given an erroneous status in the reports and logs, and the following message is displayed in the result page:

The query contains too many terms

A value lower than the default one speeds up querying (fewer terms are queried), but increases the likelihood of erroneous queries.

Note: The maximum number of terms per query must be a value between 8 and 65,536.

d. In Maximum Returned Results, you can change the maximum number of results that a query can return. Less relevant results are excluded. The default is 1000.

Consider reducing the value to speeds up querying as fewer results will be transferred to the browser. However, pertinent documents can be left out of the result list.

Note: The maximum number of returned results must be a value between 100 and 50,000.

e. In Administration Tool Language, select the language of the Administration Tool user interface.

Tip: You can also switch between user interface languages from anywhere in the Administration Tool using the Ctrl+Alt+Page Up keyboard shortcut keys.

f. CES 7.0.6884+ (May 2014) Next to Search Debugging, clear the Enable the debug query argument check box when you want to prevent displaying debug information for all search interfaces when the debug=1 argument is added to the URL of a search interface in the browser address box (see "Getting Debug Information from a .NET Search Interface" on page 135).

It is recommended to temporarily enable debug information only when you need it for troubleshooting purposes to minimize access to the potentially sensitive debug information.
8.7.5 Administration Tool - Support Tab

The Support tab contains one page that contains support links and information that are useful when you need to get help for Coveo Enterprise Search (CES).

### Available Links | Usage
--- | ---
Product home page | Reach the product page on the Coveo website
Knowledge base | Reach the Coveo Online Help
Check for Coveo Enterprise Search software updates | Reach the download page for the latest Coveo Enterprise Search version
Contact the customer support team | Reach the Coveo contact page
Open the Coveo Diagnostic Tool to help gathering troubleshooting information | Reach the Coveo Diagnostic Tool System Status tab
Upgradable License | Reach the Coveo contact page
View License Details | Reach the Administration Tool License page
8.7.6 Opening the .NET Interface Editor

You can access the .NET Interface Editor directly from a Coveo search interface or from the Coveo Front-End server.

**Note:** Only a Coveo administrator with full access or member of the Search Interface Designers role can access the .NET Interface Editor (see "About Administration Roles" on page 406 and "Assigning Users to Administration Roles" on page 412).

To open the .NET Interface Editor

- From a Coveo search interface:
  1. Open the Coveo search interface that you want to modify.
  2. At the top-right corner of the search interface, in the Do more menu, select **Edit this Interface**.

  **Note:** The Edit this Interface option appears in the Do more menu only when you have full Coveo administrator privileges or when you are a member of the Search Interface Designers role (see "About Administration Roles" on page 406 and "Assigning Users to Administration Roles" on page 412).

- From the Coveo Front-End server:
  1. Using an administrator account, connect to the Coveo Front-End server on which you want to modify a search interface.
  2. On the Windows Start menu, select All Programs > Coveo .NET Front-End 12 > Interface Editor.
  3. Select the Search Hubs tab, and in the Current Hub drop-down list on the menu bar, select the hub containing the search interface that you want to modify.
  4. Select the Search Interfaces tab, and in the Current interface drop-down list on the menu bar, select the search interface that you want to modify.

- Using the .NET Interface Editor URL:
  1. In the address bar of a browser, enter the .NET Interface Editor URL in the form:

     ![Image](image)

     **Examples:** When you are logged in to the Coveo server, use: http://localhost:8080/SearchAdmin

     From any computer, use: http://MyCoveoServer:8080/SearchAdmin


Note: If you get an error when you try to access the .NET Interface Editor from a remote computer, ensure that:

- The URL contains the appropriate port.
- The firewall on the Coveo server is allowing communications for the port.

2. In the dialog box that appears, enter your Coveo administrator user name and password, and then click OK.

8.7.7 Navigating in the .NET Interface Editor

The pages of the .NET Interface Editor are organized in a series of tabs at the top of the application. The corresponding content appears below.

When a second hierarchical level is necessary, an horizontal menu bar appears below the tabs. For the **Search Hubs** and **Search Interfaces** tabs, a drop-down list also appears at the right-end of the menu bar to allow you to respectively select the **Current Hub** or **Current Interface** to which the parameters in the selected page apply.

When a third hierarchical level is necessary, a vertical navigation panel appears on the left side of the page. The corresponding content then appears on the right side of the page.

To navigate to a specific page of the .NET Interface Editor

1. Select the appropriate tab.
2. When an horizontal menu bar appears, select the appropriate menu command.
3. For **Search Hubs** and **Search Interfaces** tabs, in the **Current Hub** or **Current Interface** drop-down list that appears at the right-end of the menu bar, respectively select the appropriate hub or search interface to which the parameters in the selected page will apply.
4. When a third hierarchical level is necessary, select the appropriate item in the navigation panel on the left side of the page.

Note: The Tab > Menu Command > Navigation Panel Item syntax is often used throughout the documentation to quickly identify the location of a page. The > symbol is used as the separator.
Example: In the .NET Interface Editor, go to the Search Interfaces > Features > General page.

1. Level 1 - Search Interfaces is selected in the series of tabs
2. Level 2 - Features is selected in the menu bar
3. The Current Interface drop-down list
4. Level 3 - General is selected in the navigation panel
5. Corresponding content

8.7.8 .NET Interface Editor - Search Hubs Tab

The Search Hubs tab of the Coveo .NET Front-End Interface Editor contains menus:

- Features menu
  
  Used to set how the search interfaces appear in the hub.

- Content menu

www.coveo.com
Used to set which search interfaces appear in a hub when accessed from the standard Web page, from a mobile device, and from Microsoft Outlook.

8.7.8.1 What Is a Search Hub?

In the Coveo .NET Front-End Interface Editor, a search hub is a single point of view grouping one or more search interfaces that appear as tabs. The Coveo Platform comes with a default search hub that offers the out-of-the-box search interfaces.

Using the .NET Interface Editor, you can:

- Select the search interfaces appearing in a hub (see "Making Search Interfaces Available in a Search Hub With the .NET Interface Editor" on page 543).
- Add a search interface to a hub and restrict who can access this search interface by assigning one or more audiences to the search interface (see "Adding Search Interfaces to a Search Hub With the .NET Interface Editor" on page 544).
- Create new search hubs (see "Creating a Search Hub With the .NET Interface Editor" on page 540).

A search hub is referenced in the default document defined in IIS for your Coveo search website but you can also use Coveo search hubs in any ASCX file (see "Integrating a .NET Search Hub in ASP" on page 145).

8.7.8.2 Creating a Search Hub With the .NET Interface Editor

The Coveo .NET Front-End comes with a default search hub. Because the default search hub configuration is overwritten when you upgrade to a new CES version or release, it is not recommended to modify and use the default search hub. You should rather create, modify, and use custom search hubs.

Example: You can create a Sales search hub that includes the People and CRM search interfaces.

To create a new search hub with the .NET Interface Editor

1. Access the Coveo .NET Front-End Interface Editor.
2. Select the Search Hubs tab.
3. On the menu, select Create a new Search Hub from the Current Hub drop-down list.
4. In the page that appears:

a. In the **Name** box, enter name for your hub. The name must not include spaces or special characters.

b. In the **Copy From** drop-down list, select the existing search hub on which the new search hub is based.

c. Click **Create**.

**What's Next?**

You may want to perform the following tasks:

- Set the general search hub parameters (see "Configuring the General Search Hub Parameters With the .NET Interface Editor" on page 549).

- Assign specific search interfaces to the new search hub (see "Making Search Interfaces Available in a Search Hub With the .NET Interface Editor" on page 543).

- Use the new search hub in an ASPX page (see "Integrating a .NET Search Hub in ASP" on page 145).

8.7.8.3 Deleting a Search Hub With the .NET Interface Editor

You may want to delete unused search hubs.

To delete a search hub with the .NET Interface Editor

1. Access the Coveo .NET Front-End Interface Editor.

2. Select the **Search Hubs** tab.

3. On the menu, in the **Current Hub** drop-down list:
a. Select the hub that you want to delete.

b. Select **Delete Current Search Hub** from the **Current Hub** drop-down list.

4. Click **Yes** at the confirmation prompt.

### 8.7.8.4 Previewing a Search Hub in a Browser With the .NET Interface Editor

You can open the available search hubs in a browser directly from the Coveo .NET Front End Interface Editor. This function is useful to easily access various hubs and see what they contain.

To preview a search hub in a browser with the .NET Interface Editor

1. Access the Coveo .NET Front-End Interface Editor.

2. Select the **Search Hubs** tab.

3. On the menu, in the **Current Hub** drop-down list:

   a. Select the hub that you want to view.

   b. Select **View Search Hub in Browser**.

      The search hub appears in the browser.

### 8.7.8.5 What Is a Search Interface?

A search interface is a single entry point providing access to the content of an index. It allows users to send queries as well as display, sort and save results.

**Note:** Coveo .NET Front-End search interfaces are Web-based, meaning that your Coveo administrator can integrate them to any of your web pages so that you can access them using any supported browser.
8.7.8.6 Making Search Interfaces Available in a Search Hub With the .NET Interface Editor

A search hub contains one or more Coveo .NET Front-End search interfaces. As a Coveo administrator, using the .NET Interface Editor, you can create a hub that contains one or more search interfaces appropriate to a specific audience of the search hub.

To select the search interfaces available in a search hub with the .NET Interface Editor

1. Access the Coveo .NET Front-End Interface Editor.
2. Select Search Hubs > Content.
3. On the menu, in the Current Hub drop-down list, select the hub for which you want to select the available search interfaces.
4. In the panel on the left, select Standard Version.

The search interfaces appearing in the list will appear in the search hub.

- To add other search interfaces, click Add (see "Adding Search Interfaces to a Search Hub With the .NET Interface Editor" on page 544).
- To remove search interfaces:
  a. Select the check box in front of one or more search interfaces that you want to remove from the search hub.
  b. Click Remove Selection.
  c. Click Yes at the question asking to confirm the search interface removal.
- To change the order in which the search interfaces appear, use the Up and Down links.
5. When needed, repeat the previous step to select available search interface when accessing the hub from:
   - Mobile devices, by clicking Mobile Version.
   - The Outlook Sidebar, by clicking Outlook version.
8.7.8.7 Adding Search Interfaces to a Search Hub With the .NET Interface Editor

A search hub contains one or more Coveo .NET Front-End search interfaces. As a Coveo administrator, you can add search interfaces to a search hub.

For each .NET search interface, you can specify if the search interface can receive or send results from/to other search interfaces of the search hub through mini queries. The mini queries appear as mini-results. You can also assign audiences to each search interface so that only members of the selected audiences have access to the search interface.

To add a search interface with the .NET Interface Editor

1. Access the Coveo .NET Front-End Interface Editor.
2. Select Search Hubs > Content.
3. On the menu, in the Current Hub drop-down list, select the hub to which you want to add a search interface.
4. In the panel on the left, select the hub version to which you want to add a search interface (Standard Version, Mobile Version, or Outlook Version).
5. Click Add.
6. Under Edit Hub Content:

   a. In the Interface drop-down list, select the search interface that you want to add to the search hub.
   b. Select the Enable mini queries from this search interface check box to allow this interface to provide search highlights to produce mini-results in other search interfaces.
   c. Select the Enable mini queries results in this search interface check box to allow displaying search highlights as mini-results from other search interfaces.
   d. Select the Overridable by Per Uri settings or query string arguments check box in cases where you
want to be able to change the search interface by passing the search interface name via a query or using per URI settings. When selected, at loading time, a search interface looks at the query string and uses the specified search interface rather than its normal configuration.

**Note:** This override is a legacy feature that was used to switch between search interfaces before search hubs where introduced. In SharePoint, it can still be useful to switch between search interfaces as a function of the SharePoint site.

e. When you want to restrict the access to this search interface to a specific group of users, in the **Available Audiences** list, select one or more audiences that are allowed to access this interface, and then click to move one or more selected audiences to the **Selected Audiences** list.

f. Click OK.

### 8.7.8.8 Enabling Mini-Results in Search Interfaces With the .NET Interface Editor

Mini-results correspond to a short list of results from a Coveo .NET Front-End search interface other than the current one. The mini-results list appears at the top of the interface, before the normal results. Mini-results are useful to expand the scope of a given search interface.

**Example:** By default, the **My Email** search interface includes mini-results from the **People** search interface.

Mini-results come from one or more search interfaces available within the current hub. Consequently, when a search hub contains only one search interface, that search interface cannot include mini-results.

In the .NET Interface Editor, you can enable for each search interface if it can send mini-results to other search interfaces and if it can receive results from other search interfaces.

**To enable mini-results in a search interface with the .NET Interface Editor**

1. Access the Coveo .NET Front-End Interface Editor.
2. Select **Search Hubs > Content**.
3. In the panel on the left, select **Standard Version**.
4. In the panel on the right, click the search interface in which you want to include mini-results.
5. Under **Edit Hub Content**:
   a. Select the **Enable mini queries results in this search interface** check box.
   b. When you want this search interface to also send mini-results to other search interfaces, select **Enable mini queries from this search interface**.
   c. Click OK.
6. Back to the previous page, click at least one other search interface from which you want mini-results to be sent.
7. Under **Edit Hub Content**:
a. Select the **Enable mini queries from this search interface** check box.

b. When you want this search interface to also include mini-results from other search interfaces, select the **Enable mini queries results in this search interface** check box.

c. Click **OK**.

### 8.7.8.9 Limiting the Quick View Size in Search Interfaces With the .NET Interface Editor

The Coveo .NET Front-End Quick View for large documents will necessarily take more space in the index and therefore take significantly more time to load when the end user clicks the **Quick View** link in the search interface.

As an administrator, you can set a limit on the size of the Quick View file that is downloaded in Coveo .NET search interfaces. The purpose of this limit is to ensure that the Quick View of large documents still appears relatively quickly. The inconvenient however is that when this limit is reached, the document displayed in the Quick View will be truncated, allowing users to only review the beginning of the document.

The **Maximum Quick View Size** parameter default value, 5 MB, should allow to display all Quick View documents within an acceptable short time, even for mobile devices or older desktop computers with limited memory. Consider increasing this value when your index contains a fair number of large documents and the Quick View truncation becomes an issue. When most devices accessing the search interface are configured with a few GB of memory, a limit of 50 MB is probably a more optimal value.

You can set the limit at the hub level to set a default size for all search interfaces in the hub, but also overwrite the limit for individual search interfaces. The limits apply to both the original and enhanced Quick Views (see "About the Enhanced Quick View" on page 470).

To limit the Quick View size in Coveo .NET search interfaces with the .NET Interface Editor

1. Access the Coveo .NET Front-End Interface Editor.

2. To set the default Quick View size limit for all search interfaces in the hub:
   a. Select **Search Hubs > Features**.
   b. In the navigation panel on the left, select **General**.
   c. In the **Quick View Settings** section:
i. In the **Maximum Quick View Size** box, enter the maximum file size, and then select the units.

ii. Click **Apply**.

3. To customize the Quick View size limit for a given search interface:
   a. Select the **Search interfaces** tab.
   b. In the upper-right corner, in the **Current Interface** drop-down list, select the search interface for which you want to set the Quick View size limit.
   c. In the menu, ensure that **Features** is selected.
   d. In the navigation panel on the left, select **General**.
   e. In the **Quick View Settings** section:
      i. Next to **Maximum Quick View Size**, select the **Custom** option.
      
      ![Quick View Settings](image)

      **Note:** Select **Inherit Hub Setting** to use the default value set at the hub level.

      ii. In the box, enter the maximum file size, and then select the units.

   f. Click **Apply**.

4. Perform tests in your environment with typical devices to evaluate the loading time for documents reaching the
8.7.8.10 Configuring a .NET Hub to Show a Drop-Down List for Overflowing Search Interface Links

In a Coveo .NET Front-End search hub, search interface links appear side-by-side on the top menu. When a hub contains a large number of search interface links or when the search interface names are long, the links may not all fit within the width of the page.

As a Coveo administrator, you can configure the hub to show a fixed number of search interfaces links on the top menu. Overflowing search interface links will then automatically appear in a drop-down list.

To configure a .NET hub to show a drop-down list for overflowing search interface links

1. Access the Coveo .NET Front-End Interface Editor.
2. In the Interface Editor, select Search Hubs > Features.
3. In the navigation panel on the left, select General.
4. Under Basic Configuration, in the Top Menu Visible Interfaces box, enter the maximum number of search interface links to appear on the top menu.

Example: When a hub contains 9 search interfaces and you only want to see the first 7 links in the top menu, enter 7. The last 2 search interface links will appear in a drop-down box.

5. Click Apply.
8.7.8.11 Configuring the General Search Hub Parameters With the .NET Interface Editor

After creating a Coveo .NET Front-End search hub or at any time later, you can set the general search hub parameters.

To configure the general search hub parameters with the .NET Interface Editor

1. Access the Coveo .NET Front-End Interface Editor.
2. Select the search hub for which you want to set general parameters:
   a. Click the Search Hubs tab, and then click the Features menu.
   b. On the menu bar, in the Current Hub drop-down list, select the hub for which you want to make changes.
3. In the navigation panel on the left, click General.
4. In the panel on the right:

   ![Image of .NET Interface Editor]

   a. Under Basic Configuration:
      i. In the Title box, enter the label for this search interface. This name appears at the top of the search interface in the tab allowing end-users to choose the interface.

         | Note: When you plan to make available multi-language search interfaces, do not forget to click the button at the end of the parameter box to open the dialog box where you can enter translations for this text strings.

      ii. In the Title Top Menu Visible Interfaces box, enter the maximum number of search interface links to
appear on the top menu in a search interface. Other search interface links appear in a drop-down list.

b. Under Position and Size:
   i. Select the **Use all available horizontal space** check box only when you want the search interfaces in the search hub to use the full width of the browser window.
   ii. With the **Use all available horizontal space** check box cleared, you can rather center the search interface content in the browser window by selecting the **Center search interface in available space** check box.

   AND

   In the **Interface Width** box, enter a fixed search interface width in pixels. The default value is 975 pixels and is appropriate to ensure that the search interface fully appears in 1024 x 768 resolution screens.

   iii. In the **Default Facet Position** drop-down list, select where the facets appear by default (**Right, Top** or **Left** zone) relative to search results for all the search interfaces in this hub.

   iv. **Coveo.NET Front-End 12.0.404+ (October 2013)** Similarly, in the **Default Related Results Position** drop-down list, select where the Related Results panels appear by default (**Right, Top** or **Left** zone) relative to search results for all the search interfaces in this hub.

c. Click **Apply**.

8.7.8.12 Configuring the Culture of a Search Hub With the .NET Interface Editor

When the end-users of your Coveo .NET Front-End search interfaces work in different languages or from different countries, you can configure some aspects of the search interfaces to adapt to their culture.

You can configure the following cultural aspects:

- The language(s) for the stemming expand of query terms.
- The language of the text elements appearing in the search interface (default, dynamically adapt to the browser language settings, custom). The Coveo search interfaces are available in several languages.
- The format of date and time values appearing in the search interface

The procedure below describes how to set culture parameters at the search hub level, thus affecting all search interfaces contained in the search hub. When needed, you can also set the culture parameters for a specific search interface to override the otherwise inherited search hub settings (see "Configuring the Culture of a .NET Search Interface" on page 596).

**Note:** You can also specify the available languages in which the search interfaces can appear (see "Configuring the Available .NET Search Interface Languages" on page 640).
To configure the culture of a search hub with the .NET Interface Editor

1. Access the Coveo .NET Front-End Interface Editor.

2. Select the search hub for which you want to globally set the language and the date/time formats:
   
   a. Click the **Search Hubs** tab, and then click the **Features** menu.

   b. On the menu bar, in the **Current Hub** drop-down list, select the hub for which you want to make changes.

3. In the navigation panel on the left, click **Culture**.

4. In the panel on the right:

   a. Under **Language Specific Query Processing**, select one of the following options to determine the language or languages used by the stemming algorithm to expand the query:

   - Automatic language selection based on index content
   - Inherit search interface language
   - All supported languages
   - Custom list of languages

   b. Under **Default culture**, select from the options:

   - Default culture
   - Client browser language preference
   - Custom

   c. Under **Date and Time Formats**, select from the options:

   - Short time format
   - Short date format
   - Long date format

   **Quick Tip**
   It is possible to use a custom culture such as en-US, fr-FR or fr-CA to display the search hub in a specific culture. For more information, [click here](#).
Automatic language selection based on index content

Expands queries only for the dominant languages detected in indexed documents. This option is useful to maximize search results for terms from the most frequent languages detected in your unified index.

Example: When the bulk of your unified index contains English, Spanish and German document, queries are expanded only using English, Spanish and German stem classes, not stem classes for other less frequent languages found in your unified index.

Inherit search interface language

Expand queries only for the language of the search interface. This option is useful to optimize search results expansion for the language of the search interface.

Example: In a global enterprise, the query of an employee using a German search interface is expanded using German stem classes. The search results will likely contain more German terms and documents compared to the same query performed from an English search interface.

All supported languages

Expand queries for all supported languages found in your unified index. This option is useful to maximize search results to all supported languages, but can produce more complex expansions and therefore increase query response time.

Custom list of languages

Always expand queries for selected languages. Select one or more languages in the Available Languages list, and then click the right-arrow to move them to the Selected Languages list.

b. Under Search Hub Culture, select one of the following options to set the default language in which the search interface text elements appear:

Default culture

With this option, the search interfaces appear in the culture specified in the web page that displays the search hub. When the web page does not specify the culture, the default culture parameters are taken from the culture settings of the web server from which the web page originates.

Example: By default, the Default.aspx file that comes with CES is the web page that displays the search hub. This file does not specify the culture (<%@ Page language="c#" %>). The search hub therefore takes the culture from the server settings.

You can also use one of the culture ready web page files to display the search hub. For example, the Default-es.aspx file specifies the Spanish culture (<%@ Page language="c#" culture="es-ES" uiCulture="ES" %>). The search hub default culture is therefore independent from the server culture settings.

Important: The Coveo search interfaces are available in several languages. When a translation for the language of the selected culture is not supported, the search interface text elements appear in English.
Client browser language preference

The search interface culture is determined by the client browser preferences. This option is useful to dynamically switch the language of the search interface to match the language in the browser of each user.

Custom

Select this option to specify a culture using the form <language_code>-<country_code>. This option is useful to force the search interface text elements to a specific language, independently from the web page, web server, or client browser settings.

Example: Enter en-GB for the Great Britain English culture.

The language is selected independently from the specified country.

Example: Entering fr-FR or fr-CA selects French as the language for search interface elements in both cases.

Note: Refer to the Microsoft National Language Support (NLS) API Reference document for a list of available culture names.

c. Under Date and Time Formats, select one of the following options to set the default formats for date and time values:

Default formats

Uses the standard formats for date and time values associated with the selected search hub culture.

Custom

Select this option to force multi-language formats for Short time format, Short date format, and Long date format using custom date/time format strings.

Example: Entering dddd, dd-MM-yyyy in Long date format displays the date 2011-01-15 as Saturday, 15-01-2011.

Click the button next to the boxes ( ) to open a dialog box where you can customize the format for each supported search interface language.
The search interface culture determines which of the format will be used.

**Example:** When the culture is **fr-FR** or **fr-CA**, the French date and time formats are used.

When the language of the search interface culture is not defined in the above dialog box, the formats associated with English are used.

**Example:** When the culture is **it-IT**, the English date and time formats are used as Italian is not a supported user interface language.

**Note:** Refer to the Microsoft **Date and Time Format Strings** document for details on standard and custom date/time format strings.

d. Click **Apply** to make changes effective for all search interfaces of the selected search hub.

5. When you want to set different language or date/time settings for a specific search interface:

a. Click the **Search Interfaces** tab, and then click the **Features** menu.

b. On the menu bar, in the **Current Interface** drop-down list, select the search interface for which you want to make changes.

c. In the navigation panel on the left, click **Culture**.

d. In the page that appears, under **Search Interface Culture**, select one of the following options to set the language in which the search interface text elements appear:

**Default culture**

With this option, the default search interface culture is inherited from the search hub settings. When the
search interface is displayed outside of a hub, the search interface appears in the language specified in the web page from which it is displayed. When the web page does not specify the culture, the culture settings are taken from the server culture settings.

Client browser language preference

The search interface culture is determined by the client browser preferences.

Custom

Select this option to specify a fix custom culture using the form `<language_code>-<country_code>`.

e. Under **Date and Time Formats**, select one of the following options to set the default formats for date and time values:

Default formats

With this option, the data and time formats are inherited from the search hub settings or, when the search interface is displayed outside of a hub, from the search interface culture.

Custom

Select this option to force multi-language formats for **Short time format**, **Short date format**, and **Long date format** using custom date/time format strings.

Click the button next to the boxes ( ), to open a dialog box where you can customize the format for each supported search interface language.

The search interface culture determines which of the format will be used. When the language of the culture is not defined in the dialog box, the formats associated with English are used.

f. Click **Apply** to make changes effective for the selected search interface.

8.7.9 .NET Interface Editor - Search Interfaces Tab

The **Search Interfaces** tab of the Coveo .NET Front-End Interface Editor contains several horizontal and vertical menus illustrated and briefly described in the following figure and table.
<table>
<thead>
<tr>
<th>Menu</th>
<th>Vertical menu</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Features</strong></td>
<td>General</td>
<td>Used to select the title, equivalent interfaces for other hub versions (standard, mobile, Outlook), and the logos for the search interface (see &quot;Changing the Logo Appearing in a Search Interface With the .NET Interface Editor&quot; on page 561).</td>
</tr>
<tr>
<td>Options</td>
<td></td>
<td>Used to activate which features pertaining to the search box, result list, displayed result elements, and result highlighting are available in the search interface (see &quot;Activating Search Interface Options With the .NET Interface Editor&quot; on page 565).</td>
</tr>
<tr>
<td>Facets and Related</td>
<td></td>
<td>Used to configure and set the position of facets and Related Results panels available in a search interface.</td>
</tr>
<tr>
<td>Results</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Culture</td>
<td></td>
<td>Used to configure the language in which the search interface appears and other cultural aspects (see &quot;Configuring the Culture of a .NET Search Interface&quot; on page 596).</td>
</tr>
<tr>
<td>Scope</td>
<td></td>
<td>Used to define the scope of the interface and define a filter that applies to the queries performed (see &quot;Configuring the Scope of a .NET Search Interface&quot; on page 597).</td>
</tr>
<tr>
<td>RSS Feeds</td>
<td></td>
<td>Used to configure the RSS options (see &quot;Specifying the RSS Feed Parameters With the .NET Interface Editor&quot; on page 601).</td>
</tr>
<tr>
<td>OpenSearch Provider</td>
<td></td>
<td>Used to publish a search provider that end-users can then define in their browser as a search engine (see &quot;Publishing an OpenSearch Provider for a Coveo .NET Search Interface&quot; on page 602).</td>
</tr>
<tr>
<td><strong>Styles</strong></td>
<td>N/A</td>
<td>Used to customize the Cascading Style Sheets (CSS) used to format elements of the search interface (see &quot;Modifying .NET Search Interface CSS Styles&quot; on page 618).</td>
</tr>
<tr>
<td><strong>Fields</strong></td>
<td>Display Fields</td>
<td>Used to add information to each result entry (see &quot;What Are Display Fields?&quot; on page 620).</td>
</tr>
<tr>
<td></td>
<td>Search Fields</td>
<td>Used to add fields to the <strong>Advanced Search</strong> page of the search interface (see &quot;What Are Search Fields?&quot; on page 621).</td>
</tr>
<tr>
<td></td>
<td>Sort Fields</td>
<td>Used to configure the search results sorting choices available to end-users in a search interface (see &quot;What Is a Sort Field?&quot; on page 624).</td>
</tr>
<tr>
<td></td>
<td>Export to Excel Fields</td>
<td>Used to select fields to include in the file created with the <strong>Export to Excel</strong> function (see &quot;Selecting Fields to Export to Excel With the .NET Interface Editor&quot; on page 626).</td>
</tr>
</tbody>
</table>
### Menu | Vertical menu | Description
--- | --- | ---
Preference Defaults |  | Used to modify the default values of user preferences (see "Modifying Default .NET Search Interface Preferences" on page 627). End-users can modify the default values.
Advanced | Alternate URIs | Used to open results using a different URI than the one indexed (see "Creating Alternate URI Rules for a .NET Search Interface" on page 630).
**Example:** You can create an alternate URI to open Microsoft Exchange emails in a Web interface instead of the native mail client.
Security Provider |  | Used to add security providers used by the search interface to retrieve documents whose security permissions are different from the Windows ones (see "Adding Security Providers to a .NET Search Interface" on page 631).
Custom Scopes |  | Legacy menu used to add a new custom search scope and to specify a filter expression for the entire scope, as well as a filter expression for every remote index in the scope (see "Configuring a Custom Scope With the .NET Interface Editor" on page 633).

### 8.7.9.1 What Are the .NET Search Interface Page Types?

The Coveo .NET Front-End search interface is a single entry point providing access to the unified index content. It allows users to perform queries as well as review, sort, open, and save results.

The Coveo .NET Front-End search interface is web-based, meaning that it can be integrated to any .aspx page and accessed through any supported browser. The following table describes the function of the four different pages available in the Coveo default web search interface.

<table>
<thead>
<tr>
<th>Page</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Initial</td>
<td>Displays a search box and links above the search box to access the Advanced Search page, Preferences page, and the Coveo online Help. This page appears when the search interface is first accessed, before any query is performed afterwards, the Search page appears.</td>
</tr>
<tr>
<td>Search</td>
<td>Contains a search box and links above the search box to access the Advanced Search page, Preferences page, and the Coveo online Help as well as facets, and search results.</td>
</tr>
<tr>
<td>Advanced Search</td>
<td>Displays advanced search parameters to refine queries without using operators or field queries.</td>
</tr>
<tr>
<td>Preferences</td>
<td>Displays options to customize the way results are queried, displayed, and opened (see &quot;Modifying Default .NET Search Interface Preferences&quot; on page 627).</td>
</tr>
</tbody>
</table>

**Note:** With the exception of the Search page, these pages can be removed in the Interface Editor (see "Activating Search Interface Options With the .NET Interface Editor" on page 565).
8.7.9.2 Creating a Search Interface With the .NET Interface Editor

You may need to create a new Coveo .NET Front-End search interface to address the needs of your organization. Using the .NET Interface Editor, you can easily add a new search interface by creating a renamed copy of an existing search interface, and then modify the newly created search interface.

To create a new search interface with the .NET Interface Editor

1. Access the Coveo .NET Front-End Interface Editor.
2. Click the Search Interfaces tab.
3. On the menu bar, in the Current Interface drop-down list, select Create a New Interface.
4. In the page that appears:
   a. In the Name box, enter the desired name for your new search interface.
      This name will not be visible to end-users. It will appear in the .NET Interface Editor as an item in the Current Interface drop-down list.
   b. In the Copy From drop-down list, select the existing search interface that is the closest to what you want for the new search interface.
   c. Click Create.
5. In the General page that appears for the newly created search interface:
a. Under **Basic Configuration**:

   i. In the **Title** box, enter the name visible to end-users for this search interface.

   ii. In the **Skin** drop-down list, select the most appropriate existing skin for the new search interface.

   **Important**: It is recommended to leave the out-of-the-box skins unmodified and rather modify copies of them to ensure that out-of-the-box skins are updated when you migrate to a newer version of Coveo .NET Front-End.

b. Under **Equivalent Interfaces**:

   i. In the **Mobile Version** drop-down list, select the corresponding search interface that should be used when accessing this interface from a mobile device.

   ii. In the **Outlook Version** drop-down list, select the corresponding search interface that should be used when accessing this interface from the Outlook Sidebar.

c. When you want to use custom icons for this interface, under **Interface Icon**, click **Change** next to each icon size, and then upload or browse to select a new icon.

d. When you want to customize or remove the logo appearing next to the search box in the search interface,
use the parameters under **Customize Logo** (see "Changing the Logo Appearing in a Search Interface With the .NET Interface Editor" on page 561).

- Click **Apply**.

**What's Next?**

- Use the .NET Interface Editor features from the **Search Interfaces** tab to customize the new search interface (see ".NET Interface Editor - Search Interfaces Tab" on page 555).
- Add the new search interface to the desired search hub (see "Adding Search Interfaces to a Search Hub With the .NET Interface Editor" on page 544).

**8.7.9.3 .NET Interface Editor - Features Menu**

This section contains topics covering all the available features of a Coveo .NET Front-End search interface.

**8.7.9.3.1 What Are Skins?**

Skins are folders containing the ASP.NET templates which define the structure of the Coveo .NET Front-End search interfaces. Coveo .NET Front-End provides several skins. Developers can create new skins by copying and editing these templates.

**8.7.9.3.2 Changing the Logo Appearing in a Search Interface With the .NET Interface Editor**

The Coveo logo appears by default on the left of the search box in the Coveo .NET Front-End search interfaces. You can change or remove the logo.

To change the logo appearing in a search interface with the .NET Interface Editor

1. Access the Coveo .NET Front-End Interface Editor.
2. Select the **Search Interfaces** tab.
3. On the menu:
   a. In the **Current Interface** drop-down list, select the interface for which you want to change the logo.
   b. Select **Features**.
4. In the navigation panel on the left, select **General**.
5. Under **Customize Logo**:
   a. Clear the **Display a logo in the search interface** check box to remove the logo.
   OR
a. Select the **Display a logo in the search interface** check box to display a logo in the search interface.

b. In the **Uri of the logo image** box, enter the path and filename of the logo to display.

   The Coveo logo appears when the box is empty.

c. In the **Logo hyperlink to** box, optionally enter the hyperlink of the site or page where users are redirected when clicking the logo.

6. Click **Apply**.

8.7.9.3.3 Adding Related Results Display Templates With the .NET Interface Editor

A Related Results panel uses a display template ASCX file to define what is rendered inside the panel. Coveo .NET Front-End comes with a default display template file for out-of-the-box .NET search interfaces (`[.NET_Front-End_Path]\Web\Coveo\Skins\[Interface_Name]\RelatedResultsDisplayTemplate.ascx`), excluding mobile .NET search interfaces.

You can duplicate and customize this file to create other display templates by modifying controls they contain and add scripts to modify their behavior (see Creating or Customizing Related Results Display Template Skin Files).
Once other display templates are available, you can use the .NET Interface Editor to add a display template to a .NET search interface so that it becomes available when you add a Related Results panel for this .NET search interface in other search interfaces.

To add Related Results display templates with the .NET Interface Editor

1. Access the Coveo .NET Front-End Interface Editor.
2. Select the **Search Interfaces** tab.
3. On the menu:
   a. In the **Current Interface** drop-down list, select the interface to which you want to add Related Results display templates.
   b. Select **Features**.
4. In the navigation panel on the left, select **General**.
5. Next to **Related Results Display Templates**, click **Add New**.
6. In the line that appears:
a. In the **Template File** drop-down list, select the desired template file that you want to make available.

**Note:** The files that appear in the **Template File** drop-down list are the Related Results display template files that are currently available in the skin folder for the currently selected interface. You must create new template files in this folder before you can select them (see Creating or Customizing Related Results Display Template Skin Files).

b. In the **Name** box, enter a name to identify the selected Related Results display template file.

7. Click **Apply**.

What's Next?

In another .NET search interface, select this display template when you add a Related Results panel for this .NET search interface (see "Adding or Customizing a Related Results Panel With the .NET Interface Editor" on page 421 of this guide).
8.7.9.3.4 Activating Search Interface Options With the .NET Interface Editor

The Coveo .NET Front-End search interfaces include many optional elements that you can activate from the .NET search interface, independently for each search interface.

To activate search interface options with the .NET Interface Editor

1. Access the Coveo .NET Front-End Interface Editor.
2. In the .NET search interface, click the **Search Interfaces** tab.
3. On the menu:
   a. In the **Current Interface** drop-down list, select the search interface for which you want to activate options.
   b. Select **Features**.
4. In the navigation panel on the left, select **Options**.

5. Select the desired options in each of the following sections describing the available options:
   - "Search Box options" on page 566
   - "Result List options" on page 568
   - "Displayed Results Elements options" on page 571
   - "Result Highlighting options" on page 573

6. Click **Apply**.

**8.7.9.3.4.1 Search Box options**

Refer to the following figure and table to understand the options available under **Search Box**.

![Diagram of Search Box options](image)

1. You can change or remove the logo (see "Changing the Logo Appearing in a Search Interface With the .NET Interface Editor" on page 561).
2. The **Advanced Search** link appears when the **Enable advanced search link** option is selected.
3. The **Preferences** link appears when the **Enable Preferences link** option is selected.
4. The **Select All** and **Clear All** controls as well as check boxes for the available collections appear when the **Display collection checkboxes** option is selected.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
</table>
| Enable the welcome search page | Select to display the initial search interface page when the user accesses the interface the first time of each session (before any query is performed) or when the user launches a query with an empty search box.  
  The initial search page presents no results and can have a different layout. This option is useful for search interfaces where it does not make sense to run a default query when a search session is initiated.  
  When this option is cleared, consider selection the **Always execute the query** option. |
<p>| Enable Preferences link        | Select to show the <strong>Preferences</strong> link above the search box. Users can then click the link to access the <strong>Preferences</strong> page where they can personalize search interface options. The Coveo administrator can also set default preferences (see &quot;Modifying Default .NET Search Interface Preferences&quot; on page 627). |</p>
<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable advanced search link</td>
<td>Select to show the Advanced Search link above the search box. Users can then click the link to access the Advanced Search page where they can build a complex query using multiple parameters.</td>
</tr>
<tr>
<td>Enable saving queries and filters</td>
<td>Select to show the Save: Query</td>
</tr>
<tr>
<td>Enable searching within results</td>
<td>Select to show the Search Within Results link at the top of the default search interface facet zone. Users can click this link to refine results starting with the current results.</td>
</tr>
<tr>
<td>Enable search as you type</td>
<td>This option only applies to Coveo search boxes integrated in SharePoint or in other types of websites. Select the option to activate the search results that appear in a drop-down list below the search box while the user types a query.</td>
</tr>
<tr>
<td>Consider operators in lowercase as words</td>
<td>By default, the terms AND, OR, NOT, and NEAR (as well as their French counter parts ET, OU, SANS, and PRES) entered both in uppercase or lowercase in the search box, are interpreted as operators. It is recommended to select this option so that these terms are interpreted as normal words when they are included in lowercase in a query.</td>
</tr>
<tr>
<td>Display collection check boxes</td>
<td>Select to show, below the search box, the Select All and Clear All controls as well as check boxes for each collection available for the current search interface. This option is useful for a search interface that searches in several collections as in the All Content search interface. The user can then see and select to which collections the query applies.</td>
</tr>
<tr>
<td>Option</td>
<td>Description</td>
</tr>
<tr>
<td>--------</td>
<td>-------------</td>
</tr>
<tr>
<td>Include interface language in score calculation</td>
<td>Select to increase the ranking of documents whose language is the same as that of the search interface. <strong>Note:</strong> The document language is one of the numerous ranking criteria. Selecting this parameter only boosts the ranking according to the weight of the language criterion. <strong>Example:</strong> When indexed documents are available in English, French, German, and Spanish, and the search interface is in German, the ranking of German documents in the search results will be increased. <strong>Note:</strong> The Coveo search interfaces are available in a few languages. The .NET search interface settings found in <strong>Search Interface &gt; Features &gt; Culture</strong> determine the language in which the search interface appears.</td>
</tr>
<tr>
<td>Use the OR operator between multiple query terms</td>
<td>When selected, the documents returned by a query must always contain at least one of the query terms (words, numbers, etc.) instead of necessarily all of them. By default, the AND operator is entered between query terms. <strong>Example:</strong> The query Coveo OR Search finds documents containing Coveo or Search, or both.</td>
</tr>
</tbody>
</table>

**8.7.9.3.4.2 Result List options**

Refer to the following figures and table to understand the options available under **Result List**.

1. **RSS** link appears when the **Enable RSS feeds** option is selected.
2. **Link** link appears when the **Enable the query link** option is selected.
3. **The Microsoft Excel XML data source** box appears when the **Enable Microsoft Excel XML data source inside the query link box** option is selected.
Messages indicating the current result refinement appear when the **Display query comments** option is selected.

Mini-results appear when results are found in other search interfaces for the current query and when the mini-result features is enabled (see "Enabling Mini-Results in Search Interfaces With the .NET Interface Editor" on page 545).

The **Export to Excel** item in the **Do more** menu appears when the **Enable exporting to Microsoft Excel** option is selected.

The **Search Within Results** link appears when the **Enable searching within results** option is selected (under **Search Box**).

The **Cluster** facet appears when the **Enable search cluster facet** option is selected.

The **Query | Filter** links appear when the **Enable saving queries and filters** option is selected (under **Search Box**).

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable search cluster facet</td>
<td>Select to make the <strong>Cluster</strong> facet appear based on results clustering (see &quot;Administration Tool - Result Clustering Menu&quot; on page 364). Users can then use this facet to refine their search results.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> Ensure that result clustering is enabled in the index before selecting this option (see &quot;Enabling and Customizing Result Clustering&quot; on page 364).</td>
</tr>
<tr>
<td>Enable RSS feeds</td>
<td>Select to make the <strong>RSS</strong> link appear at the right end of the search box panel. Users can then click the icon to subscribe to a RSS feed for specific queries.</td>
</tr>
<tr>
<td>Enable the query link</td>
<td>Select to make the <strong>Link</strong> link appear at the right end of the search box panel. Users can then click the icon to view, copy, or edit the complete query.</td>
</tr>
<tr>
<td>Option</td>
<td>Description</td>
</tr>
<tr>
<td>--------</td>
<td>-------------</td>
</tr>
<tr>
<td>Enable exporting to Microsoft Excel</td>
<td>Select to include the <strong>Export to Excel</strong> item in the <strong>Do more</strong> menu. Users can then use this menu command to export search results to the Microsoft Excel file format.</td>
</tr>
</tbody>
</table>
| Enable search highlights | **CES 7.0.7183– (November 2014)** This option is obsolete. Selecting it has no effect.  
**Note:** **CES 7.0.7256+ (December 2014)** This option is removed. |
| Display query comments | Select to display messages indicating the current refinement criteria from keywords, facets, and other refinement tools. The messages appear below the search box panel, typically in green, and include a link to clear the related constraint. This option is useful to help the user realize which refinement constraints are active.  
**Note:** The query comment feature has been replaced by the filter summary control. |
| Always execute the query | When the **Enable the welcome search page** option is cleared, select this option to ensure that the default hidden query associated with a search interface is executed when a user starts a session or initiates a search with an empty search box.  
**Example:** In the **My Emails** search interface, with this option selected, the search results can by default show the most recent email messages. |
| Filter duplicates | Select to eliminate similar results from the search result list. This option is useful to prevent viewing two or more instances of a document when copies of a document or similar documents are present in one or more indexed repositories. When this option is active and duplicate documents are filtered out, a message with a link appears at the bottom of the search interface to allow end-users to include the filtered documents in the search results. When the end-user chooses to show duplicates and duplicate documents are detected, a message with a link appears at the bottom of the search interface to allow users to hide them. This option is activated by default in several out-of-the-box search interfaces.  
**Note:** Clearing this option can reduce the query response time as search result documents would not be compared to identify duplicates at query time. |
| Enable Microsoft Excel XML data source inside the query link box | Select to include the **Microsoft Excel XML data source** box in the query link dialog box. Users can then copy the link in the box and use it in Microsoft Excel as a data source. |
| Use collaborative rating | Select to activate collaborative rating in this search interface (see "What Is Collaborative Rating?" on page 319). The three stars ★★★ appear in each result allowing users to rate documents only when the **Rating** option is selected under **Displayed Result Elements**. |
### Option | Description
--- | ---
Display Top Results icon | Select to show the star icon 🌟 to identify Top Results (see “Administration Tool - Top Results Menu” on page 312). The icon appears at the end of the title. When cleared, no icon appears and the user cannot know that the result is a Top Result.  
**Note:** Top results must be defined individually by the Coveo administrator using the Administration Tool (see “Adding Top Results to a CES Index” on page 313).

Open results in Quick View when opening in browser would not work | Select to automatically open a result in Quick View as an alternate method when the browser cannot open the document.  
This option is useful for example for file share documents that cannot be opened with all browsers without configuration or without a plug in. When the option is selected, CES detects the client browser and rather opens the result in Quick View when it determines that the browser cannot open the result directly. When the option is not selected, the user will see the browser error when the result cannot be opened.

8.7.9.3.4.3 Displayed Results Elements options

Refer to the following figure and table to understand the options available under Displayed Result Elements.

- The result number appears when the **Result number** option is selected.
- The document language appears when the **Language** option is selected.
- The date at which the document was last modified appears when the **Modified date** option is selected.
- The ranking score percentage value appears when the **Score** option is selected.
- The miniature graphical representation of the item appears when the **Thumbnail** option is selected.
- The text excerpt appears when the **Excerpt** option is selected.
- The list of concepts extracted from the document appears when the **Concepts** option is selected.
- The time elapsed since the document was last indexed appears when the **Indexed date** option is selected.
The item address appears when the **Address** option is selected.

Various contextual links appear when the **Contextual commands** option is selected.

The three stars appear to indicate and allow rating when the **Rating** option is selected.

The indication of when the item was last opened by the current user appears when the **Last click** option is selected.

The document size appears when the **Size** option is selected.

The indication of the collection and the source in which the document is indexed appears when the **Collection/source** option is selected.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Result number</td>
<td>Select to show an increasing number on the left of the result title. The number indicates the rank in the current sorting order. This option is useful when users want to precisely identify a result when scrolling back and forth in result lists.</td>
</tr>
<tr>
<td>Address</td>
<td>Select to show the URL or the path of the search result item. This option is useful when a user needs to identify the exact location of a document.</td>
</tr>
<tr>
<td><strong>Note:</strong> Users can click the ellipsis (…) to fully expand a collapsed address.</td>
<td></td>
</tr>
<tr>
<td>Excerpt</td>
<td>Select to show a text excerpt that generally contains an occurrence of the searched terms. The excerpt appears below the title. The excerpt is a very useful search result element that users can refer to evaluate the context in which search terms appear in the document. The Coveo administrator can specify the default number of excerpt lines (see “Modifying Default .NET Search Interface Preferences” on page 627). Similarly, users can personalize the number of excerpt lines.</td>
</tr>
<tr>
<td>Thumbnail</td>
<td>Select to show a miniature graphical representation of the item. The thumbnail appears on the right of the result elements to help the user to visually identify the content of the document. Thumbnails are available in Coveo results for Microsoft Office documents (when a thumbnail is included in the original document) and for supported picture file formats.</td>
</tr>
<tr>
<td>Language</td>
<td>Select to show the detected language for the document. The language identification appears at the end of the title. This option is useful when indexed repositories contain documents written in many languages to help users quickly identify the language of each document.</td>
</tr>
<tr>
<td>Last click</td>
<td>Select to show the information about when the result was last opened by the current user, from any search interface. Nothing appears when a result has never been opened by the current user. This information helps the user to identify that he previously viewed a result, and when he viewed it.</td>
</tr>
<tr>
<td>Score</td>
<td>Select to show the percentage value for the ranking score. The percentage value appears on the right end of the title line. This option is useful when results are sorted by a criterion other than relevance.</td>
</tr>
<tr>
<td>Option</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------</td>
<td>-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Size</td>
<td>Select to show the size (in bytes) of the document. The size value appears at the end of the document address line. The size value is useful to evaluate the scale of a document.</td>
</tr>
<tr>
<td>Concepts</td>
<td>Select to show the list of concepts extracted from the document. The list of concepts appears below the excerpt.</td>
</tr>
<tr>
<td>Modified date</td>
<td>Select to show the date at which the document was last modified. The date appears on the right of the title line. This option is useful to identify the freshness of the document.</td>
</tr>
<tr>
<td>Indexed date</td>
<td>Select to show the time elapsed since the document was last indexed. The information appears between the concepts and the address. This information is useful to identify the freshness of the indexed content.</td>
</tr>
<tr>
<td>Author</td>
<td>Select to show the author when available and extracted from the document metadata. The author name appears on the first line after the title.</td>
</tr>
<tr>
<td>Email (From, To, CC)</td>
<td>Select to show the From, To, and CC lines to respectively indicate the sender and recipients for email or conversation search result items. The lines appear directly under the title.</td>
</tr>
<tr>
<td>Collection/source</td>
<td>Select to show the name of the collection and source in which the document is indexed.</td>
</tr>
<tr>
<td>Contextual commands</td>
<td>Select to show various links such as Quick View and Details. The links appear on the last line. Users can click the links to trigger new result related searches. The availability of command links depends on the search interface and on the result type. Possible contextual command links are: Quick View, Details, Attachments, Emails to/from, Meetings, Contacts, Search in conversation, Folder.</td>
</tr>
<tr>
<td>Rating</td>
<td>Select to show the three stars 🌟🌟🌟 on the last line to indicate that result selection by users affect the document rating. The users can click the stars to set their personal appreciation for a result only when the Use collaborative rating option is selected under Result List.</td>
</tr>
</tbody>
</table>

8.7.9.3.4.4 Result Highlighting options

Highlighting searched terms (generally text in bold) is useful to help users to more easily locate the searched terms in various search result elements. Refer to the following table to understand the options available under Result Highlighting.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Title</td>
<td>Select to enable highlighting of searched terms in the title.</td>
</tr>
<tr>
<td>Content excerpt</td>
<td>Select to enable highlighting of searched terms in the text excerpt.</td>
</tr>
<tr>
<td>Address</td>
<td>Select to enable highlighting of searched terms in the address.</td>
</tr>
</tbody>
</table>
8.7.9.3.5 Managing Built-in Facets and Related Results Appearing in a .NET Search Interface

The Coveo .NET Front-End comes with a number of built-in facets and Related Results defined for various .NET search interfaces. You can modify which built-in facets and Related Results appear in each .NET search interface.

**Important:** The Related Results information is passed through the .NET search interface URL. When you add a few Related Results panels to a .NET search interface, the search interface URL can easily exceed the Internet Explorer URL length limit. Use the URL shortener feature to eliminate this issue.

To manage the built-in facets and Related Results appearing in a .NET search interface

1. Access the Coveo .NET Front-End Interface Editor.
2. Select the **Search Interfaces** tab.
3. On the menu bar:
   a. In the **Current Interface** drop-down list, select the search interface that you want to modify.
   b. Click the **Features** menu.
4. In the navigation panel on the left, click **Facets and Related Results**.

   In the panel on the right:
   - The facets and Related Results panels currently appearing in the selected search interface are listed under **Facets and Related Results** in the order that they appear in each of the facet and Related Results zones (Hub default position, Right, Top or Left).
   - The available built-in facets are listed under **Built-in Facets**. Several built-in facets based on system fields are applicable to content from any repository. Other facets are exclusive to the content of a specific type of repository.

     **Examples:** The **Author** facet is applicable to the content of any repository for which the `sysauthor` system field was populated. The **Liferay Type** facet is only applicable to Liferay content.

   - The available built-in Related Results are listed under **Built-in Related Results**.
5. You can perform one of the following operations:
- Add a built-in facet to the search interface:

  In the **Built-in Facets** list, click the **Add "[FacetName]"** link corresponding to the facet that you want to add.

  **Note:** For the **Type** facet, the default list of **Allowed Values** (facet items) is the following:
  audio, doc, html, image, map, mail, mime, mpp, msg, one, pdf, ppt, rtf, text, video, wp, xls, zip.

  If you want the **Type** facet to show other file types as facet items, simply add the needed file types to the default list in the **Allowed Values** parameter box.

  **Example:**
  audio, doc, html, image, map, mail, mime, mpp, msg, one, pdf, ppt, rtf, text, video, wp, xls, zip, vsd

  The corresponding facet appears at the end of the **Facets and Related Results** list.

- Add a built-in Related Results panel to the search interface:

  In the **Built-in Related Results** list, click the **Add "[RelatedResultsName]"** link corresponding to the Related Results panel that you want to add.

  The corresponding Related Results appears at the end of the **Facets and Related Results** list.

- Remove a facet or Related Results from the search interface:

  - In the **Facets and Related Results** list, select the check box of one or more facets or Related Results that you want to remove.
  
  - Click **Delete** (above the **Built-in Facets** list).
  
  - Click **Yes** when prompted to confirm the delete operation.

- Change the order in which facets and Related Results appear in the search interface:

  In the **Custom Facets** list:

  a. On the line corresponding to the facet or Related Results that you want to reorder, click **Up** or **Down** as many times as needed to relocate the facet or Related Results in relation with the others in the same zone.

  b. Repeat for each facet or Related Results that you want to reorder.

  **Note:** When the position of a facet or a Related Results panel is **Default**, the position is inherited from the search interface or search hub default position.

6. Access and refresh the search interface, and then validate that the built-in facet and Related Results changes are as desired.

8.7.9.3.6 Adding or Customizing a Facet With the .NET Interface Editor

The Coveo .Net Front-End comes with a number of built-in facets that you can easily add to your .NET search interface (see "Managing Built-in Facets and Related Results Appearing in a .NET Search Interface" on page 574).

You can also customize existing facets or create new facets and add them to a .NET search interface.
To add or customize facets with the .NET Interface Editor

1. Access the Coveo .NET Front-End Interface Editor.
2. Select the Search Interfaces tab.
3. On the menu bar:
   a. In the Current Interface drop-down list, select the search interface that you want to modify.
   b. Click the Features menu.
4. In the navigation panel on the left, click Facets and Related Results.
5. In the panel on the right:
   - To add a new facet, above the Built-in Facets list, click Add New Facet.
     
     **Note:** Creating facets by clicking Add New Facet offers more flexibility than adding built-in facets (however, built-in facets are sufficient most of the time). (see Managing Built-in Facets and Related Results Appearing in a .NET Search Interface).

     **Example:** When you create a custom facet using the sysfiletype field, you can leave the Allowed Values parameter box empty and the facet will automatically show facet items for all indexed file types. Otherwise, if you add the Type built-in facet, the facet would restrict facet items to the following values: audio, doc, html, image, mapimail, mime, mpp, msg, one, pdf, ppt, rtf, txt, video, wp, xls, zip.

     OR

   - To customize an existing facet, in the Facets and Related Results list, click the facet that you want to modify.

A page similar to the one shown below appears.
6. **Under Edit Facet**, configure the following required parameters:
a. In the Title box, type the text that you want to see as the caption at the top of the facet. Click the button to also enter the caption translated for all supported languages.

b. In the Field to Group On drop-down list, select the field whose values are used to build the items listed in the facet.

Example: Select sysauthor when you want to create a facet that lists the authors of all returned documents.

Note: When the desired field does not appear in the drop-down list, you need to make the field available using the Administration Tool (see "Adding a Facet Field" on page 500).

7. Still under Edit Facet, optionally consider changing the default behavior for the following parameters:

a. In the Field to Display drop-down list, select the field whose values are used to identify the items listed in the facet when different from the Field to Group On parameter.

Example: You can build a facet based on author IDs with the sysauthorid field but display the corresponding author names with the sysauthor field. The purpose of this procedure is to increase the precision of facet items (because each author ID is unique) without compromising their identification by users (names are more easily recognized than IDs).

b. If a developer programmed a customized version of the facet code that you want to rather use:

a. In the Assembly box, enter the fully qualified assembly name containing the class specified in the Class box.

b. In the Class box, enter the name of a class (including its namespace) to use to instantiate the facet.

c. Next to Icon, when you want to use an icon other than the default one next to the facet title:

a. Click Change.

b. Click the Choose File button that appears, and then select the icon image file in the dialog box that opens.

c. Click Upload, to transfer the file from its original location to the Coveo server.

d. In Zone, select where the facet appears in the search interface:

- Interface’s default facet position: As specified in the in Default Facet Parameter for this search interface.

- Right: Appears in the vertical zone on the right side of the search interface.

- Top: Appears in the horizontal zone at the top of the search results. This zone is generally used to host facets or Related Results panels that have a Display Style set to Dropdown.
Example:

1. A Dropdown style facet
2. The Top zone

- **Left**: Appears in the vertical zone on the left side of the search interface.

*Note*: You can hierarchically set facet positions for a hub, for a search interface, and for specific facets (see "Configuring the Position of Facets and Related Results Panels With the .NET Interface Editor" on page 591).

e. In **Display Style**, select how the facets appear:
   - **Normal**: Default format.
   - **Dropdown**: The facet appears as a drop-down control that is collapsed by default. This type of facet can only be hosted in the Top zone.

**Example**: A Source facet is illustrated below in the two formats.

- **Normal**
- **Dropdown collapsed**
- **Dropdown expanded**

*Note*: Coveo .NET Front-End 12.0.503+ (December 2013) The facet Dropdown style is reintroduced.

f. In **Display Criteria**, select the criteria determining when the facet appears:
When there is more than one result: Generally the desired behavior because a facet with one or no value is not useful to refine results.

When there is at least one result: Select when you still want to see the facet even if there is only one facet item.

Always display: Select when you always want to see the facet, even if it shows no facet item.

g. If you want to restrict facet items to specific values, in the Allowed Values box, enter a comma separated list of values. Leave the parameter empty to apply no restriction.

Example: If you wanted to create a Marketing Authors facet listing only authors from your marketing department, enter the list of marketing department employee names. The facet then only shows facet items for these authors.

h. The Performance parameter selection determines how many returned results are scanned for each query to find the possible facet items. Moving the radio button selection from the left (Faster) to the right (More Precise) increases the number of scanned results.

Selecting the left-most radio button under Faster (default value) should list all available facet items in a majority of cases since up to the first 1000 returned results are scanned to identify the possible facet items.

Try selecting a button towards More Precise when you suspect that there is a large number of facet items for this facet and you want to increase the chances that the facet displays all of them.

Selecting Most Precise ensures that the facet lists all facet items by scanning all query results. Be aware however that the facet display may be very slow with this selection for queries returning a large number of results.

Example: Let's say an Author facet appears in a search interface for a blog site with thousands of possible authors. When a query returns 80 results, the facet lists all the possible facet items. A second query returns, let's say 5000 results. In this case, because by default the facet only looks at the first 1000 returned results to identify possible authors, it is likely that the facet will not list all authors of the 5000 blog posts.

Note: The term Precision for this parameter refers to the probability for the facet to list all possible facet items. However, the number of result occurrences appearing between parentheses for each facet item is always accurate.

i. In the Number of values box, enter the number of facet items that the facet shows by default. When more facet items are available, the More control appears at the bottom of the facet to allow the user to expand the facet to show all facet items. The default value is 5.
Example: A query returns documents with a large number of different file types.

1. With **Number of values** set to 5, initially only the five most frequent file types are shown.

2. With **Additional Values Increment** set to 10, when you click More, up to ten more file types are shown.

3. With **Number of Search Values** set to 15, when you type characters in the search box, up to 15 matching items can appear in the suggestion list.

j. In the **Additional Values Increment** box, enter the number of facet items that are added/hidden each time the user clicks More/Fewer. The default value is 10.

k. In the **Number of Search Values** box, enter the maximum number of facet items that appear below the search box, in the list of facet items matching the characters typed in the search box. The default value is 15.

l. Coveo .NET Front-End 12.0.61+ (December 2012) Select the **Enable Facet Search** check box to make the search box visible.

   **Note:** The search box will not appear in the facet when you specify a field in Field to Display above.

m. In the **Dynamic Range Unit** drop-down list, when appropriate, select an option to include units to make the range values easier to read:

   - **Date:** For a facet with date range values, select to show values in the short date format (mm-dd-yyyy) rather than the long date format (mm-dd-yyyy hh:mm:ss) that appears by default.

   - **Currency:** For a facet with currency range values, select to show the values with decadic multiples of the currency (K for 1000 or M for 1,000,000).

   **Example:** $500K–$1.499M rather than $500000–$1.499999

   - **Bytes:** For a facet with file size range values, select to show values in B, KB, MB, GB, or TB units rather
than the complete integer values.

**Example:** The same File Size facet respectively when No Unit and Bytes is selected in the Dynamic Range Unit drop-down list.

n. In the Clipping Mode drop-down list, for a facet item whose length exceeds the available width in the facet, select where to truncate the text string and add the ellipsis character.

**Example:** While in most cases, it makes more sense to truncate the end of the strings, for a folder facet, it is often more useful to see the end of the path rather than the beginning.

o. In the Sort Criteria drop-down list, select the criterion controlling the order in which facet items appear:

- **Number of Occurrences:** Sorts facet items in descending order according to their number of occurrences in the search results.

  **Example:** In an Author facet, if John has written 10 documents and Jack 5, then John appears before Jack.

- **Score:** Sorts facet items in descending ranking score order. The ranking score gives more points to facet items occurring in documents appearing higher in search results. Consequently, a facet item occurring a few times in top ranking documents appears before a facet item occurring a large number of times in low ranking documents.
Example: In an Author facet, if John authored only one document but his document is one of the top ranking documents, and Jack authored 200 documents but are ranked low in the search results, then John appears before Jack in the list of facet items.

- **Ascending Alphabetical**: Sorts facet items in ascending alphabetical (A to Z) or numerical order.
- **Descending Alphabetical**: Sorts facet items in descending alphabetical (Z to A) or numerical order.
- **Correlation**: Sorts facet items based on the correlation to the current query using a chi-square method. Items that are particularly related to the query versus the rest of the index appear higher.

Example: You can use the Correlation option to sort an Expert facet to list people that are particularly related to the queried terms, not just people that are the author of many documents containing the terms.

p. Besides Depends On, select whether the appearance of this facet is conditional to another facet being used by a user. This feature is useful when the refinement criteria of two facets are linked following a hierarchy.

Example: When a search interface has both a Year facet and a Month facet, it often makes sense to only show the Month facet after the user has selected a year in the Year facet. To obtain this behavior, for the Month facet, beside Depends On select the Year check box.

q. Select the Collapse by default check box when you want the facet to initially show only its caption, not facet items.

This option is useful for example for less frequently used facets when your search interface includes many facets and you want to save vertical space.

8. Optionally, you can set what icon images appear on the left of each facet item:

a. For legacy facets only, in Default Image, enter the path and file name for the image to display as the default icon on the left of all facet items. You can specify the full path in the http://mysite.com/[path]/[image_file] form or the relative path from where the search interface page is stored.

Example: For an Author legacy facet, enter the path and file name for the icon using the full path (ex.: http://mysite.com/icon-author.png) or the relative path (ex.: ~/Coveo/Skins/MySearchInterface/icon-author.png).

b. You can also assign custom icons and captions to specific facet item values:
i. Next to Value to Image Mappings, click Add New.

Three boxes appear where you can specify one or more rules to map icons and captures to facet values.

ii. In the box on the left, type the value of the facet item to which you want to assign a specific icon and/or caption.

iii. In the box in the center, enter the path and file name for the image to display as the icon. You can specify the full path in the http://mysite.com/[path]/[image_file] form or the relative path from the search interface skin folder in the ~/[Relative_Path]/[Filename] form.

iv. In the box on the right, enter a custom caption for the item value.

**Note:** As done for some out-of-the-box facets like the Type facet, you can use an embedded resource (like coveo_embedded_res(Coveo.CES.Web.Search.Images.author.png)) or set a callback method (like callback(Coveo.CES.Web.Search.Interfaces.ValueMappingFormatter.GetFileTypeIconUri)) to dynamically get the appropriate facet item icon and caption. Entering a * in the box on the left indicates that these resources or callbacks apply to all items. This feature can be used by the Coveo Professional Services and developers.

**Example:** For a document Type facet, you may want to use specific icons and captions for Word and Excel documents and use the standard icons and captions for other file types. You can do that by entering the mappings as follows.

<table>
<thead>
<tr>
<th>Value to Image Mappings (Add New)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Word</td>
</tr>
<tr>
<td>Excel</td>
</tr>
<tr>
<td>*</td>
</tr>
<tr>
<td>value</td>
</tr>
</tbody>
</table>

9. Under Computed Fields, you can optionally configure the facet to calculate and show one or more numerical values for each facet item:

**Note:** You need a Coveo license that allows computed facets to use this feature.

a. For each computed value, click Add New next to Computed Fields.

b. In the Field drop-down box, select the field which values you want to use as the source for the calculation.

c. In the Operation drop-down box, select the mathematical operation to perform on the field values (Sum, Average, Minimum, or Maximum).

d. In the Result Display Location drop-down box, select where the calculated value appears in relation with the facet item (Beside the Caption or Under the Caption).

e. In the Result Prefix and Result Suffix boxes, if needed, respectively type the desired prefix and suffix to
appear before and after the calculated values.

For a multi-lingual search interface, click ![ellipsis icon] next to the box to open the dialog box where you can type the translated prefix or suffix for each supported language.

f. In the **Format** drop-down box, select the numerical format with which the calculated value appears in the facet (Currency, Integer, Numeric, Percentage, or Custom). When you select Custom, another box appears where you can enter the desired .NET numerical format string.

**Note:** Refer to the [Standard Numeric Format Strings MSDN documentation](https://docs.microsoft.com/en-us/dotnet/standardecosystem/standard-numeric-format-strings) for details on the .NET numeric format string.

g. When you include more than one calculated value, click **Up** or **Down** on the corresponding line, to set in which order the calculated values appear.

h. Click **Delete** on the corresponding line when you want to eliminate a calculated value.

**Example:** You could create a Document Average Size facet in which you see the average file size and the average number of pages for each document type. When it is not possible to calculate a value, like the average number of pages for HTML documents, nothing appears.

<table>
<thead>
<tr>
<th>Field</th>
<th>Operation</th>
<th>Result Display Location</th>
</tr>
</thead>
<tbody>
<tr>
<td>@size</td>
<td>Average</td>
<td>Beside the Caption</td>
</tr>
<tr>
<td>Result Prefix</td>
<td></td>
<td></td>
</tr>
<tr>
<td>@pages</td>
<td>Average</td>
<td>Under the Caption</td>
</tr>
<tr>
<td>Result Prefix</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

![Computed Fields](image)

10. Click **OK** to complete the custom facet creation.
11. Back in the Facets page, the new facet appears at the end of the Facets and Related Results list where you can:
   a. Click Up or Down to set the position of the facet relative to other facets, for each zone in the search interface.
   b. When you want to eliminate a facet, select a facet and then click Delete.

12. Using a browser, open or reload the search interface to verify that the facet behaves as you expect.

8.7.9.3.7 Adding or Customizing a Related Results Panel With the .NET Interface Editor

The Coveo .NET Front-End comes with a number of built-in Related Results panels that you can easily add to your .NET search interface (see "Managing Built-in Facets and Related Results Appearing in a .NET Search Interface" on page 574).

You can also customize existing Related Results panels or create new ones and add them to a .NET search interface.

**Important:** The Related Results information is passed through the search interface URL. When you add a few Related Results panels to a .NET search interface, the search interface URL can easily exceed the Internet Explorer URL length limit. Use the URL shortener feature to eliminate this issue (see "Deploying the .NET Search Interface URL Shortener Database" on page 124).

To add or customize a Related Results panel with the .NET Interface Editor

1. Access the Coveo .NET Front-End Interface Editor.
2. Select the Search Interfaces tab.
3. On the menu bar:
   a. In the Current Interface drop-down list, select the search interface that you want to modify.
   b. Click the Features menu.
4. In the navigation panel on the left, click Facets and Related Results.
5. In the panel on the right:
   - To add a new Related Results panel, above the Built-in Facets list, click Add New Related Results.
   - OR
   - To customize an existing Related Results panel, in the Facets and Related Results list, click the Related Results panel that you want to modify.

A page similar to the one shown below appears.
6. Under **Edit Related Results**, configure the following required parameters:

   a. In the **Title** box, type the text that you want to see as the caption at the top of the Related Results panel. Click the *** button to also enter the caption translated for all supported languages.

   b. In the **Search Interface** drop-down list, select the search interface from which you want this Related Results panel to display search results.

   c. In the **Display Template** drop-down list, select the desired Related Results display template from those available for the selected source search interface (see "Adding Related Results Display Templates With the .NET Interface Editor" on page 562).

   d. If a developer programmed a customized version of the Related Results code that you want to rather use:

      a. In the **Assembly** box, enter the fully qualified assembly name containing the class specified in the **Class** box.

      b. In the **Class** box, enter the name of a class (including its namespace) to use to instantiate the Related Results instead of the default `RelatedResultsFacet` class. The class you specify must inherit from `RelatedResultsFacet`. 
e. Next to Icon, when you want to use an icon other than the default one next to the Related Results title:
   a. Click Change.
   b. Click the Choose File button that appears, and then select the icon image file in the dialog box that opens.
   c. Click Upload, to transfer the file from its original location to the Coveo server.

f. In Zone, select where the Related Results panel appears in the search interface:
   - Interface's default related results position: As specified in the in Default Related Results Parameter for this search interface.
   - Right: Appears in the vertical zone on the right side of the search interface.
   - Top: Appears in the horizontal zone at the top of the search interface.
   - Left: Appears in the vertical zone on the left side of the search interface.

   **Note:** You can hierarchically set Related Results panel positions for a hub, for a search interface, and for specific Related Results panels (see "Configuring the Position of Facets and Related Results Panels With the .NET Interface Editor" on page 591).

g. In Display Style, select the how the Related Results panel appear:
   - Normal: Default format.
   - Dropdown: The Related Results panel appears as a drop-down control that is collapsed by default. This type of Related Results panel is generally hosted in the Top Zone.

h. In the Number of Results box, enter the number of search results that appear in the panel. The default value is 3.

i. In the Sort Criteria drop-down list, select the criterion controlling the order in which search results appear in the Related Results panel following:
   - Default: Default sort option set for the related search interface
     When you change the sort option for the search interface, the sort option also changes for the Related Results panel.
   - Relevance: Descending ranking score order
   - Modified Date Ascending: Modified date, starting with the oldest.
   - Modified Date Descending: Modified date, starting with the newest.

j. Select the Collapse by default check box when you want the Related Results panel to initially show only its caption, not search results.
This option is useful for example for less frequently used Related Results panels when your search interface includes many Related Results panels and you want to save vertical space.

7. You can modify the ranking score of search results appearing in the Related Results panel using query ranking expressions (see "What Are Query Ranking Expressions?" on page 612):

   a. Next to Query Ranking Expressions, click Add New.

   ![Query Ranking Expressions](image)

   b. In the Expression box, enter a valid query ranking expression (QRE).

   c. In the Modifier drop-down list, select the appropriate modifier value.

   **Note:** CES 7.0.8388+ (June 2016) Once done, ensure query expressions (QREs) are effective by reviewing the Ranking weights tab of any search result. The tab shows the weight of each QRE that impacted the ranking of a result (see Troubleshooting Ranking).

8. Click OK to complete the custom Related Result panel creation.

9. Back in the Facets and Related Results page, the new Related Result panel appears at the end of the Facets and Related Results list where you can:

   a. Click Up or Down to set the position of the Related Result panel relative to other Related Result panels and facets, for each zone in the search interface.

   b. When you want to eliminate a Related Result panel, select a Related Result panel and then click Delete.

10. Using a browser, open or reload the search interface to verify that the Related Result panel behaves as you expect.
Note: You can also add a Related Results panel in a search interface by editing its skin. Facets and Related Results are typically defined in the `leftToolbar.ascx` and `RightToolbar.ascx` files.

Example: The following code shows a Related Results control inserted in one of those files:

```xml
<ces:RelatedResultsFacet InterfaceName="People" DisplayTemplateAscxFilename="RelatedResultsDisplayTemplate.ascx" ID="rrfPeople" Title="Related People" SortBy="ModifiedDateAscending" NumberOfResults="5" FacetId="MustHaveAUniqueIdHere" runat="server" />
```

8.7.9.3.8 Configuring the Position of Facets and Related Results Panels With the .NET Interface Editor

The Coveo administrator can configure where each facet or Related Results panel appears in the Coveo .NET Front-End search interface. In a .NET search interface, facets and Related Results panels can appear vertically stacked on either sides, or at the top of search results.

Example: In the following example, a few facets appear in the left zone, one appears in the Dropdown format in the top zone, and one Related Results panel appears in the right zone.

You can manage the position of the facets and Related Results panels globally for a .NET search hub. Each search interface of the hub can inherit or overwrite the hub default facet Related Results panel position.

Similarly, each facet and Related Results panel in a .NET search interface can inherit or overwrite the default search interface facet and Related Results panel position. You can configure facets and Related Results panels to also appear in the top horizontal zone but only at the facet level.
To configure the position of facets and Related Results panels with the .NET Interface Editor

1. Access the Coveo .NET Front-End Interface Editor.

2. To configure the default facet and Related Results panel position at the hub level:
   a. Select the Search Hubs tab.
   b. On the menu bar, in the Current Hub drop-down list, select the hub for which you want to configure the default facet position.
   c. In the navigation panel on the left, select General.
   d. In the Default Facet Position drop-down list, select the desired default zone (Right, Top or Left) where facets will appear by default for the search interfaces of this hub.
   e. Similarly, in the Default Related Results Position drop-down list, select the desired default zone (Right, Top or Left) where Related Results panels will appear by default for the search interfaces of this hub.
   f. Click Apply.

3. To configure the default facet and Related Results panel position at the search interface level:
   a. Select the Search Interfaces tab.
   b. On the menu bar, in the Current Interface drop-down list, select the search interface for which you want to configure the default positions.
   c. On the menu, select Features.
   d. In the navigation panel on the left, select Facets and Related Results.
   e. In the Default Facet Position drop-down list, select the desired zone where facets will appear by default in this search interface.
      - Choose Hub default facet position when you want to use the facet position configuration set at the hub level. This option is useful to easily and globally change the position of facets from the hub level.
      - Choose Right, Top or Left when you want to customize the default facet position for this search interface.
   f. Similarly, in the Default Related Results Position drop-down list, select the desired zone where Related Results panels will appear by default in this search interface.

4. To customize the position of a specific facet or Related Results panel:
   a. Select the Search Interfaces tab.
   b. On the menu bar, in the Current Interface drop-down list, select the search interface containing the facet or Related Results panel for which you want to configure the position.
   c. On the menu, select Features.
   d. In the navigation panel on the left, select Facets and Related Results.
In the panel on the right, under **Facets and Related Results**, click the facet or Related Results panel for which you want to customize the position.

a. In the **Zone** drop-down list, select the desired facet zone where you want this facet or Related Results panel to appear.

- Choose **Interface’s default facet/related results position** when you want to easily and globally change the position from the search interface level.
- Choose **Right** or **Left** when you want to only customize the position of this facet or Related Results panel.
- Choose **Top** to make the facet appear at the top of search results.

b. Click **OK**.

**Note:** While the search interface is loaded in a browser, a Related Results panel can disappear or keep its old settings when you make customization in the Interface Editor, even after refreshing the page.

These issues may occur because the state of the Related Results panels is saved in the page URL hash. Restart your browser or, in the address bar, delete the URL segment starting with the # character.

### 8.7.9.3.9 Tuning the Facet Performance Parameter With the .NET Interface Editor

In most cases, the Coveo .NET Front-End default facet configuration efficiently produces a facet with a complete list of facet items. For facets which could contain a large number of items, the default configuration may produce facets that do not list all possible facet items. When this is not acceptable, consider tuning the facet performance parameter available in the .NET Interface Editor.

**To tune the facet performance parameter with the .NET Interface Editor**

1. Access the Coveo .NET Front-End Interface Editor.

2. Select the **Search Interfaces** tab.

3. On the menu bar:
   a. In the **Current Interface** drop-down list, select the search interface that you want to modify.
   b. Click the **Features** menu.

4. In the navigation panel on the left, click **Facets and Related Results**.

5. In the right panel, under **Facets and Related Results**, click the facet for which you want to tune the performance.

6. Next to **Performance**:

<table>
<thead>
<tr>
<th>Performance</th>
<th>Faster</th>
<th>Slower</th>
<th>Slowest</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td><img src="less_precise_icon" alt="Less Precise" /></td>
<td><img src="more_precise_icon" alt="More Precise" /></td>
<td><img src="most_precise_icon" alt="Most Precise" /></td>
</tr>
</tbody>
</table>

Choose one of the available options to set how many returned results are scanned for each query to find the possible facet items. Moving the option selection from the left (Less Precise) to the right (More Precise) increases the number of scanned results.

- Selecting the left-most option under Faster (default value) should list all available facet items in a majority of cases since the facet display process scans up to the first 1000 returned results to identify the possible facet items.
- Select a button towards More Precise when you suspect that there is a large number of facet items and you want to increase the chances that the facet displays all of them.
- Selecting Most Precise ensures that the facet lists all items by scanning all query results. Be aware however that with this selection, the facet display may be very slow for queries returning a large number of results.

Example: Let's say an Author facet appears in a search interface for a blog site with thousands of possible authors. When a query returns 80 results, the facet lists all the possible facet items. A second query returns, let's say 5000 results. In this case, because by default the facet only looks at the first 1000 returned results to identify possible authors, it is likely that the facet will not list all authors of the 5000 blog posts.

Note: The term Precision for this parameter refers to the probability for the facet to list all possible facet items. However, the number of result occurrences appearing between parentheses for each facet item is always accurate.

7. Click OK.

8.7.9.3.10 Configuring a Computed Facet With the .NET Interface Editor

Using the Coveo .NET Front-End Interface Editor, a Coveo administrator can configure a computed facet when creating a new facet, or as described in the following procedure, modifying an existing facet.

To configure a computed facet with the .NET Interface Editor

1. Access the Coveo .NET Front-End Interface Editor.
2. Select the Search Interfaces tab.
3. On the menu bar:
   a. In the Current Interface drop-down list, select the search interface that you want to modify.
   b. Click the Features menu.
4. In the navigation panel on the left, click Facets and Related Results.
5. In the right panel, in the list under Facets and Related Results, click the existing facet that you want to modify.
6. For each computed value that you want to add to the facet, next to Computed Fields, click Add New.
   New parameters appear below Computed Fields.
In the **Field** drop-down box, select the field whose values you want to use as the source for the calculation.

b. In the **Operation** drop-down box, select the mathematical operation to perform on the field values (*Sum*, *Average*, *Minimum*, or *Maximum*).

c. In the **Result Display Location** drop-down box, select where the computed value appears in relation with the facet item (**Beside the Caption** or **Under the Caption**).

d. In the **Result Prefix** and **Result Suffix** boxes, if needed, respectively type the desired prefix and suffix to appear before and after the computed values.

For a multi-lingual search interface, click next to each box to open the dialog box where you can type the translated prefix or suffix for each supported language.

e. In the **Format** drop-down box, select the numerical format in which the computed value appears in the facet. The available options are:

   - **Currency**: Presents the value as an integer (no decimal digits). Separators appear when the value exceeds groups of three digits (for example: $2,104,542). The currency symbol ($) automatically appears before the value.

   - **Numeric (Integer)**: Presents the value as an integer (no decimal digits). Separators appear when the value exceeds groups of three digits (for example: 6,542).

   - **Numeric (Floating point)**: Presents the value with two decimal digits and separators appear when the value exceeds groups of three digits (for example: 6,542.19).

   - **Percentage**: Presents the value with two decimal digits and the percent symbol (%) automatically appears after the value (for example: 92.03 %).

   - **Custom**: When you select **Custom**, another box appears where you can enter the desired .NET numeric format string.

   **Note**: Refer to the [Standard Numeric Format Strings](https://docs.microsoft.com) MSDN documentation for details on the .NET numeric format string.
Example: You could create a **Document Average Size** facet in which you see the average file size and the average number of pages for each document type as shown in the following figures.

<table>
<thead>
<tr>
<th>Field</th>
<th>Operation</th>
<th>Result Display Location</th>
</tr>
</thead>
<tbody>
<tr>
<td>@syssize</td>
<td>Average</td>
<td>Beside the Caption</td>
</tr>
</tbody>
</table>

**Computed Fields (Add New)**

<table>
<thead>
<tr>
<th>Field</th>
<th>Format</th>
<th>Result Suffix</th>
</tr>
</thead>
<tbody>
<tr>
<td>Result Prefix</td>
<td>Integer</td>
<td>bytes</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Field</th>
<th>Operation</th>
<th>Result Display Location</th>
</tr>
</thead>
<tbody>
<tr>
<td>@syspages</td>
<td>Average</td>
<td>Under the Caption</td>
</tr>
</tbody>
</table>

**Document Average Size**

<table>
<thead>
<tr>
<th>Format</th>
<th>Result Suffix</th>
</tr>
</thead>
<tbody>
<tr>
<td>Avg</td>
<td>pages</td>
</tr>
</tbody>
</table>

**Note:** When it is not possible to calculate a value, like the average number of pages for HTML documents, the value and its prefix and suffix simply do not appear.

7. When you include more than one computed value, click **Up** or **Down** on the corresponding line to set in which order the computed values appear.

8. When you want to remove a computed value, click **Delete** on the corresponding line.

9. Click **OK** to complete the custom facet modification.

10. Using a browser, open or reload the search interface to verify that the facet includes the computed values you configured.

### 8.7.9.3.11 Configuring the Culture of a .NET Search Interface

When the end-users of your Coveo .NET Front-End search interfaces work in different languages or from different countries, you can configure some aspects of the .NET search interfaces to adapt to their culture.
It is recommended to first set culture parameters at the .NET search hub level as this configuration is inherited by all .NET search interfaces contained in the .NET search hub (see "Configuring the Culture of a Search Hub With the .NET Interface Editor" on page 550).

When needed, you can also use the following procedure to access the page where you can set culture parameters for a specific search interface and override the otherwise inherited .NET search hub settings.

To configure the culture of a .NET search interface

1. Access the Coveo .NET Front-End Interface Editor.
2. Click the Search interfaces tab.
3. On the menu bar:
   a. In the Current Interface drop-down list, select the search interface for which you want to make changes.
   b. Select the Features menu.
4. In the navigation panel on the left, click Culture.
5. In the panel on the right, under Language Specific Query Processing, clear the Inherit hub language check box to be able to customize the settings for this interface.

The rest of the panel is identical to the one used to set the search hub culture. Refer to the topic for this page for details on how to set the culture parameters (see "Configuring the Culture of a Search Hub With the .NET Interface Editor" on page 550).

8.7.9.3.12 Configuring the Scope of a .NET Search Interface

You can configure the scope of a Coveo .NET Front-End search interface using one or more of the following methods to transparently restrict the results for all queries performed from this .NET search interface:

- Hidden search filters
- Selection of one or more index collections
- Inclusion of one or more search scopes defined on the Coveo Master server (see "What Are Search Scopes?" on page 360 and "Adding a Search Scope" on page 361).

To configure the scope of a .NET search interface

1. Access the Coveo .NET Front-End Interface Editor.
2. Select Search Interfaces > Features.
3. In the Current Interface drop-down box, select the search interface for which you want to configure the scope.
4. In the navigation panel on the left, select Scopes.
5. In the page that appears in the right panel, use one or more of the following steps to configure the scope of the search interface:
a. In the **Hidden search filter** box, optionally enter a filter expression using search features such as field queries.

**Example:** For a **My Email** search interface returning results from a Microsoft Exchange server, a hidden query could restrict results to each user mailbox and exclude certain types of documents to present only email messages applicable to the current user:

```plaintext
@sysmailbox=="username@MyOrganization.com" @sysfiletype<>exchangeappointment
@sysfiletype<>exchangetask @sysmailbox @sysfiletype>
(activatedirperson,csuser,exchangeperson,mergedperson,msdcontact, sblcontact,sfcontact,suserprofile) @sysfiletype<>exchangecalendarmessage
@sysfiletype<>exchangerssfeed
```

**Note:** The end-user does not see this filter in the search box but can see it using the Link link when it is available.

b. Under **Available Collections**, optionally select the check box for one or more collections in which the search will be performed.

**Examples:**

- For a **My Email** search interface, you could select one or more collections containing email and mail archives content.
- For an **All Content** search interface, you could select all available collections.

c. Under **Scope Configuration**, when you want to include one or more search scopes defined on the Coveo Master server:
Select the **Use the Default Scope from the Administration Tool** option, to follow the default search scope defined from the Administration Tool (see "Setting a Default Search Scope" on page 363).

OR

i. Select the **Select Scopes from the Administration Tool** option.

   ii. In the drop-down list, select one of the search scopes available from the Coveo Master server, and then click **Add**.

   **Note:** When the drop-down list is empty, you must first centrally define search scopes using the Administration Tool (see "Adding a Search Scope" on page 361).

   iii. Click the **Translation** link to enter a localized name for this search scope in the other supported languages (see "Configuring the Available .NET Search Interface Languages" on page 640).

   iv. Optionally add other search scopes and then use the **Up** and **Down** links to set the order in which the search scopes appear in the **Search In** facet.

   v. Select the check box in front of one added search scope and then click **Set as Default** when you want this search scope to be automatically selected in the **Search In** facet when an end-user accesses the search interface for which you are configuring the scope.
When more than one Coveo instance exists within your organization (see "About Geographically Distributed Indexing" on page 20), you can also optionally add one or more remote indexes to the scope of the search interface:

i. Next to **Additional Indexes To Include In Default Search**, click **Add New**.

   **Note:** You can click **Add New** only when at least one remote index is defined in the Administration Tool for the current Coveo instance (see "Adding or Modifying Remote Indexes" on page 355).

ii. From the **Name** drop-down list, select the remote index from which you want to receive results for the current search interface.

iii. Optionally, in the **Filter Expression** box, enter a filter expression in the form of a query to add to every query sent to the remote index.

iv. In the **Time to execute (sec)** box, enter the maximum time to wait for the query results from the remote index. A warning message appears in the search interface when the time out is reached. The default value is 0, in which case the search interface waits indefinitely.

   **Note:** When the remote Coveo instance is down, local search results are presented immediately without waiting for remote results.

   **Example:** You can enter 3 (sec) to prevent the search interface from freezing when the WAN connection to the remote index is overloaded, delaying the return of the remote search results.

   **Important:** When you do not select all available collections under **Available Collections**, a hidden collection filter is generated and also applied to remote indexes. In this case, the remote indexes will only return results from collections with the same name. When remote indexes do not have the same collection names, no results will be returned. To prevent this hidden collection filter, select all collections.

d. Click **Apply**.

A message appears at the top of the page when the modifications are effective.

**Note:** CES 7.0.5556–(June 2013) You can also use the deprecated custom search feature. A custom scope is visible to end-user as an option in the **Search In** facet (see "Configuring a Custom Scope With the .NET Interface Editor" on page 633).
8.7.9.3.13 Specifying the RSS Feed Parameters With the .NET Interface Editor

This topic describes how to specify the parameters to configure the RSS feed feature for a Coveo .NET Front-End search interface to allow users to receive results through RSS feeds.

**Note:** The RSS feed feature is optional. You need to select the Enable RSS feeds option in the .NET Interface Editor for a specific .NET search interface for the RSS link to appear in the search box panel (see "Activating Search Interface Options With the .NET Interface Editor" on page 565).

To specify the RSS feed parameters with the .NET Interface Editor

1. Access the Coveo .NET Front-End Interface Editor.
2. Select Search Interfaces > Features.
3. In the panel on the left, select RSS Feeds.
4. In the RSS Feeds page:
   a. In the Title box, enter a descriptive name for the feed.

   By default, the title is Search Results for [QueryExpression], where [QueryExpression] is replaced by the last expression searched by the user. If you want to automatically include the Query Expression in your title, use the $query$ keyword.

   **Example:** Type RSS Feed for my "$query$" query.

   b. In the Description box, specify the content of the feed. If you want to automatically include the Query Expression in your title, use the $query$ keyword. Leave the box empty for no description.

   c. In the Time to live box, specify the number of minutes during which a feed can be cached before being refreshed from the source. A value higher than 60 minutes decreases bandwidth usage; whereas, a lower value increases the refresh rate of the feed. Leave the box empty for no time to live.

   d. In the Maximum results returned box (default is 100), specify the maximum number of results returned each time the feed is refreshed.

   e. Select the Include author name in results information check box, to add the document author name in the feed result information. The author name does not appear when the check box is cleared.

   f. Select the Include author name after the excerpt in results description check box to display the document author name after the corresponding excerpt.
8.7.9.3.14 Publishing an OpenSearch Provider for a Coveo .NET Search Interface

The Coveo administrator can publish an OpenSearch provider document for a Coveo .NET Front-End search interface to allow end-users to access the .NET search interface directly from the built-in search box of their web browsers.

To publish an OpenSearch provider for a Coveo .NET search interface

1. Access the Coveo .NET Front-End Interface Editor.
2. Select Search Interfaces > Features.
3. In the Current Interface drop-down box, select the interface for which you want to publish an OpenSearch provider.
4. In the navigation panel on the left, select OpenSearch Provider.
5. In the **Name** box, enter a descriptive name that clearly identifies your Coveo search interface.

   This is the name that appears in the list of available search engines in the browsers.

6. In the **Description** box, optionally enter more information describing the search interface associated with this OpenSearch provider.

7. Click **Apply**.

8. Let your end-user know that they can access the Coveo search interface from the search box of their browser.

### 8.7.9.3.15 Displaying the Query Link Icon in a .NET Search Interface

The **Link** link is a Coveo .NET Front-End optional feature that needs to be enabled by the Coveo administrator to appear in a .NET search interface.

To display the query link icon in a .NET search interface

1. Access the Coveo .NET Front-End Interface Editor.

2. Select **Search Interfaces > Features**.

3. In **Current Interface**, select the interface in which you want the **Link** link to appear.

4. In the navigation panel on the left, select **Options**.

5. Under **Result List**, select the **Enable the query link** check box.

6. Click **Apply**.

   The **Link** link appears at the right of the search box panel.

### 8.7.9.3.16 Configuring Query Completions in .NET Search Boxes

In a Coveo .NET Front-End search interface, you can configure and activate the query completion feature by adding code to the CoveoSearch.ascx file associated with a skin. The query completion configuration applies to all Coveo search boxes appearing in .NET search interfaces using the skin.

You can configure the query completion to use one or more of the following providers.
**FileCompletionProvider**

Query completion suggestions are taken from a flat completion text file stored in the skin folder. The completion file must contain one suggestion per line. A suggestion may contain many words. Ensure to save the file using the UTF8 encoding to ensure that special characters such as accented ones are rendered correctly.

The default file name is `completions.txt`, but you can use a different file name using the `FileName` attribute.

Order in which suggestions appear below the Search box:

1. Suggestions where the entered query matches the beginning of the first term in the suggestion sorted alphanumerically.
2. Suggestions where the entered query matches the beginning of other terms in the suggestion sorted alphanumerically.

**Tip:** In a document repository, useful query completion suggestions are the titles of documents available in the repository. For repositories with relatively static content and no restriction to who can see titles for all documents, you can easily create a file containing the list of titles for all documents in a repository. In a .NET search interface for this repository, run the `@uri` query to return all documents. Export the search results to an Excel file. Copy the Title column content to the `completions.txt` file.

**FieldCompletionProvider**

Query completions suggestions are taken from the list of available fields when the user types `@` optionally followed by other letters to refine the list of suggestions.

Once a string type facet enabled field is selected followed by the equal symbol, query completion suggestions are taken from matching field values (see "Adding a Facet Field" on page 500).

You can define aliases so that the user does not need to enter the `@sys` part of the field name.

You can also specify a default field (for string type facet enabled fields only), so that the user does not have to enter the field name at all. The suggestions are taken directly from the default field values.

Order in which suggestions appear below the search box:
1. Suggestions where the entered query matches the beginning of the first term in the suggestion sorted by:
   a. Decreasing number of occurrences
   b. Alphanumerical order
2. Suggestions where the entered query matches the query anywhere in the suggestion again sorted by:
   a. Decreasing number of occurrences.
   b. Alphanumerical order

**Examples:** When the user types the beginning of a field name like @sys1, the suggestions match available field names. The user can then select a string type facet field like @syslanguage, add an equal symbol (=), and start adding characters to get suggestions for matching field values.

With the field alias definition `<ces:FieldAlias Alias="Concept" Field="@sysconcepts" />`, the user can type Concept: in the search box and start adding characters to get suggestions for matching field values.

With the @sysconcepts field set as the default field, the suggestions directly match document concepts.

**EmailCompletionProvider**

Query completion suggestions are taken from sender/recipient email fields (to, from, cc, bcc).

The user gets suggestions for a specific field by typing a field alias followed by a colon character, and then typing the first characters of the name.
Order in which suggestions appear below the search box:

1. Suggestions where the entered query matches the beginning of the first term in the suggestion sorted by:
   a. Decreasing number of occurrences
   b. Alphanumerical order
2. Suggestions where the entered query matches the query anywhere in the suggestion again sorted by:
   a. Decreasing number of occurrences.
   b. Alphanumerical order

Note: The EmailCompletionProvider is activated by default in the out-of-the-box My Emails .NET search interface.

AnalyticsCompletionProvider

Query completion suggestions are taken from queries in the search history of the Usage Analytics Module.

You can configure the scope of the suggestions to be for past queries:

- Entered by all users versus only the current user (using the LimitToCurrentUser attribute).
- Entered in any .NET search interface versus only in the current search interface (using the LimitToCurrentInterface attribute).

No suggestions are presented when the Usage Analytics Module is not active (see "Deploying the On-Premises Usage Analytics Module" on page 651).

Suggestions where the entered query matches the beginning of the first term in the suggestion are sorted by:

1. Decreasing number of occurrences.
2. Alphanumerical order.

Note: The AnalyticsCompletionProvider is activated by default in all the out-of-the-box .NET search interfaces except My Emails.
MetaCompletionProvider

Query completion suggestions are mixed from two or more completion providers.

You can use providers of the same or of different types but mixing disparate suggestion types may be confusing for the end-user.

The order in which suggestions appear below the search box depends on the type of completion providers that are used.

To configure and activate query completions in a .NET search interface

1. On the Coveo Master server, open the folder corresponding to the skin used by the .NET search interface for which you want to enable the query completions (#.NET_Front-End_Path\Web\Coveo\Skins\[Search_Interface_Skin]).

   You can find the skin used by a .NET search interface from the .NET Interface Editor (Search Interfaces tab > Features menu > General page).

   **Example:** The folder for the skin used by the My Email .NET search interface is typically in C:\Program Files\Coveo .NET Front-End 12\Web\Coveo\Skins\Email.

2. Using a text editor:
   a. Open the CoveoSearch.ascx file found in the skin folder.
   b. After the ASP.NET directives and before the user control HTML markup, add one of the following completion provider element:
Example: The following code sample shows the default CoveoSearch.ascx file for the Default skin. Notice the location of the `<ces:FieldCompletionProvider...>` element.

```csharp
<%@ Control Language="c#" AutoEventWireup="false" Inherits="Coveo.CES.Web.Search.Controls.SearchControl" %>

<ces:FieldCompletionProvider id="fcp" BindTo="Interface" DefaultField="@systitle" runat="server" />

<%--
 This user control defines the look and structure of the CES search interface.

**************************************************************************
* This user control defines the look and structure of the CES search interface.
**************************************************************************-
%>

<div class="CesSearch">
<ces:SearchUpdatePanel id="mup" BlankOnHistory="true" runat="server">
    <ces:LoadIfActive Path="TopMenu.ascx" WithID="t" runat="server"/>
    <ces:LoadIfActive Path="InitialPanel.ascx" WithID="i" runat="server"/>
    <ces:LoadIfActive Path="SearchPanel.ascx" WithID="s" runat="server"/>
    <ces:MainUpdatePanel runat="server">
        <ces:LoadIfActive Path="ResultsPanel.ascx" WithID="rs" runat="server"/>
        <ces:OpenSearchProvider runat="server"/>
        <ces:SearchBar runat="server"/>
        <ces:DebugInfo runat="server"/>
    </ces:MainUpdatePanel>
</ces:SearchUpdatePanel>
</div>
```

- **FileCompletionProvider** element:

  ```csharp
  <ces:FileCompletionProvider id="fcp" BindTo="Interface" runat="server" FileName="[MyCompletionFile].txt" />
  ```

  where you replace `[MyCompletionFile]` by the name of your custom text file, or simply omit the `FileName` optional attribute to use the completions.txt default file name.

  **Important:** The text file containing the completions must be stored in the same skin folder.

- **FieldCompletionProvider** element:

  ```csharp
  <ces:FieldCompletionProvider id="fcp" BindTo="Interface" runat="server" DefaultField="@systitle" />
  ```

  where the optional `FieldCompletionProvider` attribute is:

  **DefaultField**

  Specifies the CES field to use by default for the source of completions when no other field or alias is explicitly specified by the user.

  You can also include optional aliases as follows:

  ```csharp
  <ces:FieldCompletionProvider id="fcp" BindTo="Interface" runat="server">
    <Aliases>
        <ces:FieldAlias Alias="Author" Field="@sysauthor" />
        <ces:FieldAlias Alias="Type" Field="@sysfiletype" />
    </Aliases>
    <ces:FieldCompletionProvider>
  ```
where the optional **FieldAlias** attributes are:

**UseAlias**

Set this attribute to `True` so that after selecting a suggestion, the alias appears in the search box rather than the corresponding field name (ex.: `Concept` not `@sysconcept`). A CES alias with the same name must exist for the same field. Omit or leave this attribute to `False`, the default value, when no CES alias is defined to prevent the occurrence of errors.

**IsPreloaded**

Set this attribute to `True` to load the field values in cache memory when the search session starts to prevent having to wait for the suggestion list to appear. Be aware that a field with a large number of values can take a significant amount of cache memory. The default value is `False`.

- **EmailCompletionProvider** element:

  ```xml
  <ces:EmailCompletionProvider id="emcp" BindTo="Interface" runat="server"/>
  ```

- **AnalyticsCompletionProvider** element:

  ```xml
  <ces:AnalyticsCompletionProvider id="ancp" BindTo="Interface" runat="server"
  LimitToCurrentUser="True" LimitToCurrentInterface="True" CompletionTimeout=2 />
  ```

where the optional **EmailCompletionProvider** attributes are:

**LimitToCurrentUser**

Set by default to `True` to limit the completion scope to past queries entered by the current user. Set to `False` to expand the completion scope to past queries entered by all users.

**LimitToCurrentInterface**

Set by default to `True` to limit the completion scope to past queries entered in the current .NET search interface. Set to `False` to expand the completion scope to past queries entered in any .NET search interface.

**LookForPrefixInsideQueries**

Set by default to `False` to only return suggestions matching the first term of the suggestions. Set to `True` to return suggestions matching the beginning of terms anywhere in the suggestions.

**CompletionTimeout**

Set by default to 30 seconds, the maximum time the query completions function waits for suggestions from the Usage Analytics Module.

- **MetaCompletionProvider** element:
Example: To use two different FileCompletionProvider files:

```xml
<ces:MetaCompletionProvider id="mcp" BindTo="Interface" runat="server">
  <ces:FileCompletionProvider id="fcp1" FileName="ACompletionFile.txt" runat="server" />
  <ces:FileCompletionProvider id="fcp2" FileName="AnotherCompletionFile.txt" runat="server" />
</ces:MetaCompletionProvider>
```

where the optional MetaCompletionProvider attribute is:

**CompleteWithNext**

Set by default to **False** to stop calling sub-completion providers as soon as one provider returns at least one completion. Set it to **True** to force the meta completion provider to continue to get completions until it reaches the maximum number of results defined by the `MaxCompletions` attribute.

**Note:** The completion providers declared inside a `MetaCompletionProvider` element should not include a `BindTo` attribute. These attributes are ignored if present.

c. For all completion providers, you can use the following optional attributes:

**Note:** You can omit optional attributes to automatically use the default value.

**MaxCompletions**

Determines the maximum number of suggestions to display below the search box. The default value is 10.

**CompletionMaxLength**

Determines the maximum number of suggestion characters to show. When the length of a suggestion exceeds the maximum value, the end of the suggestion text is truncated and replaced by an ellipse ("..."). When a truncated suggestion is selected, a tooltip appears to show the complete suggestion text. This parameter is useful to prevent line wrapping for long suggestions. The default value is 45.

**Example:** Customizing the maximum number of suggestions and the maximum number of characters in a suggestion.

```xml
<ces:FileCompletionProvider id="fcp" BindTo="Interface" runat="server" MaxCompletions="20" CompletionMaxLength="30" />
```

**QueryFormat**

Allows to customize the query sent to CES based on the text entered by the user using the `%Value%` token.
Example: You configured the FileCompletionProvider with a file that contains author names but you want to automatically create a @author field query with the selected suggestion. To do so, you can configure the completion provider as follows:

```xml
<ces:FileCompletionProvider id="fcp" BindTo="Interface" QueryFormat='@sysauthor="%VALUE%"' runat="server" />
```

When the selected suggested value is John Smith, the resulting query that appears in the search box is @sysauthor="John Smith" rather than just John Smith, ensuring that only documents with this field value are returned, not any documents containing John Smith.

It is recommended to enclose the replacement value with quote marks to prevent breaking suggestions containing spaces, and consequently enclose the QueryFormat value with single quotes as follows:

Example: QueryFormat='"@author="%VALUE%""

Note: You can also bind a completion provider to a hub (BindTo="Hub") so that search boxes in all .NET search interfaces in the hub inherit the completion provider. A completion provider BindTo="Interface" declaration in a skin overwrites the hub bound completion provider for search boxes in a .NET search interfaces using this skin. You can also bind a completion provider to a specific control, which overwrites a skin bound completion provider.

d. The suggestion matching characters are highlighted in bold by default in the suggestion list but you can customize the highlighting appearance by adding to the CoveoSearch.ascx file the CSS classes shown in the following example, and adapt the CSS code as you wish.

Example: With the CSS classes:

```css
<style type="text/css">
 .CnlAutoCompleteDropdownItem span
 {
  color: red;
 }

 .CnlAutoCompleteDropdownItemSelected span
 {
  color: blue;
 }
</style>
```

When the user types jo, the span section in the <span>Jo</span>hn <span>Sm</span>ith suggestion appears in red in the list and in blue when the mouse is over the suggestion.

e. Save the changes to the file.

Note: By default, the provider waits for 250 mS after a user starts typing to get and propose suggestions. The provider does not wait for a minimum number of characters. You can change the delay by adding the attribute TypingDelay="500" in the <ces:query/> control in the skins (InitialPanel and SearchPanel). The provider waits for that number of milliseconds after the last keystroke to fire the AJAX call to get the completions.

3. Clear the cache of your browser and reload the .NET search interface page to validate that the query

www.coveo.com
completion suggestions are available in the search box.

8.7.9.3.17 What Are Query Ranking Expressions?

A query ranking expression (QRE) modifies the ranking score of search results matching a query expression. QREs are implemented by administrators or developers for a given search interface when they want to adjust how search results are ranked.

A QRE consists of:

- Any valid query expression
  
  One or many terms and one or many operators supported by Coveo Enterprise Search (CES), including date queries, Boolean queries, field queries, etc.

- A ranking modifier
  
  A value that either boosts or decreases the ranking score of documents that match the query expression.

  **Note:** The QRE modifier value is correlated to the final search results ranking score by a 1 to 10 ratio.

  **Example:** A QRE is made of the `@author="Barack Obama"` query expression and the +10 modifier value. In search results, all documents for which Barack Obama is the author will have 100 added to their normal ranking score. The ranking score of returned documents with other authors is not affected.

You can implement one or more QREs in a given context. There are no hard limits to the number of QREs that can be evaluated, although implementing several may have an impact on search interface performances.

8.7.9.3.17.1 QRE Usage Example

In a search interface that has a large scope, QREs can boost search results matching your relevance criteria, but still return results from the whole scope, as opposed to reducing the scope of the search interface to show only the more relevant content.

  **Example:** The search interface of an Engineering department Intranet site has a scope that includes the Intranet content (source named Intranet_Eng), but also other Engineering documents repositories. This large scope is useful as engineers can search all Engineering content from one place. However, because they search from the Intranet, they are likely to be looking primarily for content from the Intranet.

  If you want to favor search results from the Intranet in this search interface, you can define a QRE with the query expression `@source="Intranet_Eng"` and a modifier of +50 to boost the ranking of Intranet search results and provide better contextual search results.

8.7.9.3.17.2 What Is the Impact of Modifier Values on the Final Ranking Score?

QREs should use a modifier between -100 and +100 to alter ranking without completely overriding it. A match for a document and QRE using a modifier of 100 gives approximately the same score bonus as a non-frequent term matching a title.
8.7.9.3.17.3 How to Implement QREs?

- An administrator can add QREs to specific search interfaces from the Interface Editor for a search interface (see "Customizing the Ranking for a .NET Search Interface" on page 613) or for a Related Results panel (see Adding or Customizing a Related Results Panel With the .NET Interface Editor).

- A developer can implement QREs programmatically (see Adding Query Ranking Expressions to a Search Interfaces).

8.7.9.3.18 Customizing the Ranking for a .NET Search Interface

The Coveo Platform uses sophisticated search results ranking algorithms to return the most relevant documents for each query. There are several ways that you can use to optimize the ranking of your search results (see "Best Practices for Ranking Optimization" on page 317).

Coveo .NET Front-End 12.0.360+ (September 2013) One way to adjust the ranking is for a given Coveo .NET Front-End search interface. From the .NET Interface Editor, you can assign one or more query ranking expressions (QRE) to a .NET search interface to promote or demote the ranking of documents matching a given query (see "What Are Query Ranking Expressions?" on page 612).

To customize the ranking for a .NET search interface

1. Access the Coveo .NET Front-End Interface Editor.

2. Click the Search interfaces tab.

3. On the menu bar:
   a. In the Current Interface drop-down list, select the search interface for which you want to adjust search results ranking.
   b. Select Features.

4. In the navigation panel on the left, select Ranking.

5. In the panel on the right:
a. Click **Add New**.

b. In the **Expression** box, enter the valid query expression that returns the documents for which you want to modify the ranking score.

   **Note:** The expression is not validated by the front-end. If it is invalid, it will be ignored by the index and the message will be generated. It is therefore recommended that you test your expression. You can simply enter it in the search box of the interface, verify that it is valid and that it returns the expected documents.

c. In the **Modifier** drop-down list, select a preset modifier value, or select **Custom**, and then enter the desired value that must be between -100 and +100 (see "What Is the Impact of Modifier Values on the Final Ranking Score?" on page 612).

   **Note:** By default, the modifier values are limited to be between -100 and +100 to ensure that your QRE does not completely override the normal ranking algorithm. You can however disable this restriction by setting the `limitQueryRankingExpressionsModifierRange` option to **false** in the [.NET_Front-End_Path]\Web\Web.config file.

   ```xml
   <coveoEnterpriseSearch>
   <database ... />
   <analytics ... />
   <server ... />
   <options ... limitQueryRankingExpressionsModifierRange="false" ... />
   </coveoEnterpriseSearch>
   
   By default, the `options` tag is not present in the `coveoEnterpriseSearch` section of the `Web.config` file. You must also ensure that the following element is present in the `<sectionGroup name="coveoEnterpriseSearch">` section:

   ```xml
   <section name="options" type="System.Configuration.SingleTagSectionHandler, System, Version=1.0.3300.0, Culture=neutral, PublicKeyToken=b77a5c561934e089" />
   
   You will then be able to enter values ranging from -2,147,483,648 to +2,147,483,647.
   
   d. Click **Apply**.

   6. Repeat the previous step to add another QRE to this interface.

   7. In the search interface, perform queries to validate that the QRE addition produces the desired search results ranking adjustments.

8.7.9.3.19 Configuring Query Suggestions for Scarce Results in a .NET Search Interface

The Coveo .NET Front-End out-of-the-box search interfaces feature query suggestions when a query returns no or only a few results. Query suggestions can be of different types. A query suggestion indicates the type, the number of results, and optionally sample results.
The query suggestion proposition

The number of returned results

Optional sample results

Note: The feature is available and activated by default in most out-of-the-box .NET search interfaces but not mobile .NET search interfaces.

8.7.9.3.19.1 Query Suggestions Skin Templates

The query suggestion is defined in ASCX files in the respective skin folders. The query suggestion skin template location and content varies depending on the type of skin.

Normal skin

The query suggestion template for all .NET search interface skins is located in the ResultsPanel.ascx file after the <ces:NoResultsAdvices> section.

```
<%-- Query suggestions are displayed when there are few or no results --%>
<ces:QuerySuggestions id="sug" CssClass="CesQuerySuggestions" DisplaySampleResults="True" runat="server">
  <SuggestionTemplate>
    <div class="CesQuerySuggestion">
      <ces:QuerySuggestionLink runat="server" />
      <ces:QuerySuggestionSampleResults runat="server">
        <SampleResultTemplate>
          <ces:DefaultResultTemplate TemplatePath="SuggestionSampleResult.ascx" runat="server"/>
          </SampleResultTemplate>
        </ces:QuerySuggestionSampleResults>
      </div>
    </SuggestionTemplate>
  </ces:QuerySuggestions>
```

Outlook skin

The query suggestion template for the Outlook skin is located in the CoveoSearch.ascx file in the <ces:IfNoResults> section. In this skin, query suggestions will only be shown if there are no results returned. Sample results are disabled by default in Outlook skins.

```
<%-- Query summary (only if no results) --%>
<ces:IfNoResults runat="server">
  <ces:QuerySummary id="$Prefix$qsm" CssClass="CesQuerySummary" runat="server" />
  <ces:NoResultsAdvices CssClass="CesNoResultsAdvices" style="margin-top: 10px;" runat="server" />
Console skin

The query suggestion template for the console skin used in the Account Console and Case Console search interfaces is located in the MasterSection.ascx file after the <aes:NoResultsAdvices> section.

Mobile skin

The query suggestions are not available in the mobile skin templates.

8.7.9.3.19.2 Customizing Query Suggestions

As an administrator, you can customize a few aspects of the query suggestion feature by editing the skin templates.

To customize the query suggestions

1. Using an administrator account, connect to your Coveo Front-End server.

2. Navigate to the skin folder for the .NET search interface that you want to modify ([.NET_Front-End_Path]\Web\Coveo\Skins\{search_interface}).

3. Using a text editor:
   a. Open the ASCX file containing the query suggestion template (see "Query Suggestions Skin Templates" on page 615).
   b. Edit the file to perform one or more of the following possible customization.
      - Change the maximum number of returned results that triggers the query suggestions:

         In the <aes:QuerySuggestion> tag, add the FewResults="n" attribute to set the returned result count below or equal to n for which the query suggestion feature looks for alternate queries. The default value is 5 when not specified.

         - Display or not sample results
In the `<ces:QuerySuggestion>` tag, add the `DisplaySampleResults="true"` attribute to make sample results appear. The default is `false` when not specified. The maximum number of sample result is also customizable.

**Example:**

```
<table>
<thead>
<tr>
<th></th>
<th>Main part of the suggestion presenting the alternate query and indicating the number of returned results (always present)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Search instead for collection permission modify policy object (6 results)</td>
</tr>
<tr>
<td></td>
<td>List of Acronyms</td>
</tr>
<tr>
<td></td>
<td>Collaborative Data Objects, an application programming interface included...</td>
</tr>
<tr>
<td>2</td>
<td>Configuring the Desktop Integration Package GPO</td>
</tr>
<tr>
<td></td>
<td>In the Group Policy Object (GPO), you can configure three Desktop Integration...</td>
</tr>
<tr>
<td></td>
<td>8/24/2012</td>
</tr>
</tbody>
</table>
```

- **Change the number of sample results to display per query suggestion**
  
  In the `<ces:QuerySuggestion>` tag, add the `NumberOfSampleResults="n"` attribute to set the number of sample results to display. The default value is `2` when not specified.

- **Change the maximum number of query suggestions to try**

  In the `<ces:QuerySuggestion>` tag, add the `QueryLimit="n"` attribute to set the maximum number of alternative queries tested by the query suggestion feature. The default value is `5` when not specified. Avoid a large number to prevent flooding the index.

- **Change how suggested queries are sorted**

  When more than one query is suggested, the suggestions are sorted based on the number of results they return. In the `<ces:QuerySuggestion>` tag, add the `SortAscending="True"` attribute to sort starting with suggestions returning the smallest number of results. The default is `False` when not specified.

  c. Save the file.

4. You can also customize what is displayed for each result. Using a text editor:

   a. Open the `SuggestionSampleResult.ascx` template file.
   
   b. Edit the file to modify, add, or remove elements.

   **Example:** To modify the `<ces:ResultExcerpt ... />` element, refer to the API reference document to search and see available attributes (see `ResultExcerpt Class Properties`).

   c. Save the file.

5. Using a browser, access the modified .NET search interface and perform queries to validate that the changes are as expected.
8.7.9.4 .NET Interface Editor - Styles Menu

This section contains a topic explaining what a Coveo Platform administrator can do to modify the look and feel of a Coveo .NET Front-End search interface with CSS styles.

8.7.9.4.1 Modifying .NET Search Interface CSS Styles

The Coveo .NET Front-End search interfaces use Cascading Style Sheets (CSS) to format the .NET search interface elements. The styles are preconfigured for out-of-the-box .NET search interfaces, but you can modify them to adjust the look and feel of the .NET search interface.

Under the hood, the .NET Interface Editor stores the search interface CSS parameters in the [.NET_Front-End_Path]\Web\Coveo\Skins\[Skin_Name]\CoveoSearch.css file, independently for each search interface.

**Note:** For more information about CSS styles, refer to the following website page: [http://www.w3.org/Style/CSS](http://www.w3.org/Style/CSS).

To modify .NET search interface CSS styles

1. Access the Coveo .NET Front-End Interface Editor.
2. Click the Search Interfaces tab.
3. On the menu bar:
   a. In the Current Interface drop-down list, select the search interface that you want to modify.
   b. Click the Styles menu.

The page presents the complete list of all CSS styles used in the search interface.
4. In the list of styles, locate the style that you want to modify.

**Tip:** Use browser developer tools to inspect the search interface element that you want to modify and get its CSS class name. In the list of styles, lookup the class name in the **Current Styles** column.

5. Click **Edit Style** next to the style that you want to modify.

6. In the **Edit Style** page for the selected style:

   ![Edit Style Page](image)

   a. In the available CSS parameters, enter the appropriate values for the aspects that you want to modify.

   b. In the **Custom Styles** box, you can type one or more valid CSS styles that are not available from the parameters of the page.

   c. Click **OK**.

**Note:** A **Defaults** link appears next to the **Edit Style** link when a style has been modified so that you can easily revert the configuration back to the default values. The default CSS values are stored in the [.NET_Front-End_Path]\Web\ Coveo\Skins\[Skin_Name]\ CoveoSearchDefaults.css file.

8.7.9.5 .NET Interface Editor - Fields Menu
This section defines the different field types that can be added to the Coveo .NET Front-End search interface to improve end-users search experience.

The Search Interface > Fields > Facets navigation panel item allowing you to configure facets has been relocated to the Search Interface > Features > Facets and Related Results (see ".NET Interface Editor - Features Menu" on page 561).

8.7.9.5.1 What Are Display Fields?

The label and the value of a display field can appear in the search results of an out-of-the-box .NET search interface. As a Coveo administrator, using the .NET Interface Editor you can quickly add display fields to search results to provide additional information and help users identify documents that they are looking for (see "Adding Display Fields to Search Results With the .NET Interface Editor" on page 620).

By default, in the out-of-the-box .NET search interfaces, display fields appear in a smaller font at the end of the search result but before the link elements.

**Example:** In a search interface for a CRM system like Salesforce, you can set the sfcompetition field as a display field to include the competitive information in the search result. A user can see the competitors identified for a sales opportunity without having to open the search result.

![Example](image)

**The sfcompetition display field with the Competition label lists the identified competitors for this opportunity**

8.7.9.5.2 Adding Display Fields to Search Results With the .NET Interface Editor

In a Coveo .NET Front-End search interface, display fields provide additional information concerning each search result (see "What Are Display Fields?” on page 620). By default, all system fields and new custom fields that you create are set as display fields in the index so they are available from the .NET Interface Editor to be included as Display Fields in the search results of a given .NET search interface. Display fields also appear in the Index Browser which is useful for troubleshooting purposes.

**Note:** Fields are available as Display Fields in the .NET Interface Editor only when they are set as display fields in the index.

To add a display field to search results with the .NET Interface Editor

1. Access the Coveo .NET Front-End Interface Editor.
2. Select the Search Interfaces tab.
3. In the **Current Interface** drop-down list, select the interface for which you want to add a display field.

4. Select the **Fields** menu.

5. In the navigation panel on the left, select **Display Fields**.

6. Next to **Additional Fields to Display with Results**, click **Add New**.

7. Under **Edit Display Field**:

   ![Image of Edit Display Field](image)

   a. In the **Title** box:
      
      i. Enter an English label to identify the field.
      
      This label appears in the search results.
      
      ii. Click the button next to the box to open a dialog box where you can enter the label translated for the other supported languages.
      
   b. In the **Field to Display** drop-down list, select the field that you want to add as a display field.
      
   c. In the **Maximum Length** box, enter the maximum number of characters to display.
      
   d. Click **OK**.

8. Under **Additional Fields to Display with Results** you can:

   - Modify the display order of the fields by clicking the **Up** and **Down** links.
   
   - Remove display fields by selecting them and clicking **Delete**.

**8.7.9.5.3 What Are Search Fields?**

Search fields are fields that are available in the **Advanced Search** page of the default web .NET search interface. The **Advanced Search** page provides an easier interface to help users build more complex queries without having to enter operators or field queries in the search box.
With the .NET Interface Editor, you can add other search fields that will automatically appear at the end of the Document Properties section (see "Adding Search Fields With the .NET Interface Editor" on page 623).
Example: In the My Email .NET search interface, you can add the `syscc` and `sysbcc` fields to allow users to respectively specify Carbon Copy and Blank Carbon Copy email recipients in their advanced search.

8.7.9.5.4 Adding Search Fields With the .NET Interface Editor

You can add custom search fields to the Coveo .NET Front-End search interface Advanced Search page to help end-users build more complex queries without having to enter operators or field queries.

To add a search field with the .NET Interface Editor

1. Access the Coveo .NET Front-End Interface Editor.
2. Select the Search Interfaces tab.
3. In the Current Interface drop-down list, select the interface for which you want to add a search field.
4. Select the Fields menu.
5. In the navigation panel on the left, select Search Fields.
6. Next to Fields to Use to Perform Advanced Search, click Add New.
7. Under Edit Search Field:
a. In the **Title** box:
   i. Enter the English text that appears as the label for this custom search field in the **Document Properties** section of the **Advanced Search** page.
   ii. Click the **...** button next to the box to open a dialog box where you can enter the label translated for the other supported languages.

b. In the **Field to Search On** drop-down list, select the field that you want to add.

   **Note:** When the desired field does not appear, you must configure it to be searchable (see "Adding a Field to Search On" on page 499).

c. Click **OK**.

8. Under **Fields to Use to Perform Advanced Search**, you can modify the display order of the fields by clicking the **Up** and **Down** links. You can also remove fields by selecting them and clicking **Delete**.

### 8.7.9.5.5 What Is a Sort Field?

Sort fields allow end-users to modify the display order of documents in the search results.

In the Coveo .NET Front-End built-in search interfaces, the sorting criterion is available at the top of the search results with the **Sort By** control.

By default, results are ordered by relevance score (**Relevance**) or creation/modification date (**Date**). You can add other sorting parameters to a .NET search interface using the .NET Interface Editor (see "Adding Sort Criteria With the .NET Interface Editor" on page 624).

### 8.7.9.5.6 Adding Sort Criteria With the .NET Interface Editor

By default, Coveo .NET Front-End search results are ordered by relevance score or modification date. However, you can create other sorting criteria.
Example: In a .NET search interface for a CRM system such as Salesforce, you can use the `syssfpriority` field to sort sales opportunities by priority.

To add a sort field with the .NET Interface Editor

1. Access the Coveo .NET Front-End Interface Editor.
2. Select the **Search Interfaces** tab.
3. In the **Current Interface** drop-down list, select the interface for which you want to add sort criteria.
4. Select the **Fields** menu.
5. In the navigation panel on the left, select **Sort Fields**.
6. Next to **Fields to Use for Sorting**, click **Add New**.
7. Under **Edit Sort Field**:
   
   ![Edit Sort Field](image)

   a. In the **Title** box:
      
      i. Enter the English text that appears as the **Sort By** criteria label at the top of the search results in the search interface.

      ii. Click the button next to the box to open a dialog box where you can enter the label translated for the other supported languages.

   b. In the **Field to Sort On** drop-down list, select the field on which to perform the sorting.

      **Note:** When the field on which you want to perform the sort does not appear in the drop-down list, you must first make it available to sort on (see "Adding a Sorting Field" on page 502).

   c. Select the **Sort in descending order** check box to sort in the reverse order by default.

      **Note:** In the search interface, the end-users can always click the label to change the sort order.

   d. Click **OK**.
8.7.9.5.7 Selecting Fields to Export to Excel With the .NET Interface Editor

For a given Coveo .NET Front-End search interface, you can select which fields are included in the file created when end-users transfer search results to a Microsoft Excel file using the Export to Excel function.

To select fields to export to Excel with the .NET Interface Editor

1. Access the Coveo .NET Front-End Interface Editor.

2. Select the Search interfaces tab.

3. On the menu, in the Current Interface drop-down list, select the search interface for which you want to make changes.

4. First ensure that the Export to Excel function is enabled for this interface:
   a. On the menu, select Features.
   b. In the navigation panel on the left, select Options.
   c. Under Result List, select the Enable exporting to Microsoft Excel check box.
   d. Optionally, also select the Enable Microsoft Excel XML data source inside the query link box check box to be able to dynamically link search results to an Excel file from the query link dialogue box.
   e. Click Apply.

5. On the menu, select Fields.

6. In the navigation panel on the left, select Export to Excel Fields.

7. To exclude fields from the exported Excel files:
Under **Fields to Display in the Export to Excel File**, select the check box of one or more fields that you want to remove.

b. Click **Delete**.

c. Click **Yes** at the confirmation prompt.

8. To add fields to include in the exported Excel files:

- To include an existing field, under **Built-in Fields**, click one of the available **Add "[Field_Name]"** links.

OR

- To add a new field, click **Add New**, and then under **Edit Export to Excel Field**:

  a. In the **Title** box, enter the label that you want for this field. Use the button to open the dialog box where you can set the label for all supported languages.

  b. In the **Field to Display** drop-down list, select the desired field.

  c. Select the **Display as a Link** check box when you want the field to be an hyperlink in the Excel file.

  d. Click **OK**.

9. Optionally, select the **Include document real path in the exported fields** check box to include the path to the documents in the Excel files.

8.7.9.6 .NET Interface Editor - Preference Defaults Menu

This section contains a topic describing how to modify the default Coveo .NET Front-End search interface preferences for all end-users using the .NET Interface Editor.

8.7.9.6.1 Modifying Default .NET Search Interface Preferences

The **Preference Defaults** page of the Coveo .NET Front-End Interface Editor corresponds to the **Preferences** page of the .NET search interface. As the Coveo administrator, you can use the **Preference Defaults** page to adjust the default values of the .NET search interface preferences for all users. Each user can subsequently modify each of these values.
User preferences are stored in browser cookies which contain only the variation between default and user-selected values. This method applies new default values instantaneously for all users without affecting user customized values.

Notes:

- You must select the **Enable Preferences link** option in the .NET Interface Editor to make the **Preferences** link appear above the search box for a specific search interface (see "Activating Search Interface Options With the .NET Interface Editor" on page 565).
- You can configure preferences to be saved in a user profile database rather than in browser cookies, making end-user preferences available from any browser and device even when cookies are not allowed or deleted (see [Enabling a User Profile Database](#)).

To modify the default value of user preferences

1. Access the Coveo .NET Front-End Interface Editor.
2. Select the **Search Interfaces** tab.
3. On the menu bar:
   a. In the **Current Interface** drop-down list, select the search interface that you want to modify.
   b. Click the **Preferences Default** menu.
4. In the **General Preferences** page, edit the available options.
For more information on each parameter, refer to the following table.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Number of results per page</td>
<td>Specifies the number of results that appear on each search results page.</td>
</tr>
<tr>
<td>Number of lines in excerpt</td>
<td>Specifies the number of lines to include in the text excerpt for each result.</td>
</tr>
<tr>
<td>Initialize the Mailbox facet using your default mailbox</td>
<td>When selected, specifies your default mailbox as the active filter for the Mailbox facet. Select this option for the My Email search interface. When cleared, the Mailbox facet shows all mailboxes to which you have access.</td>
</tr>
<tr>
<td>Always open results in new window</td>
<td>When selected, CES opens documents that you click in search results in a new browser window. When cleared, CES opens the document in the same window as the result list.</td>
</tr>
<tr>
<td>Use wildcard queries</td>
<td>When selected, * and ? characters entered in the search box are interpreted as wildcard operators.</td>
</tr>
<tr>
<td>Use thesaurus for automatic query expansion</td>
<td>When selected, CES checks if keywords in the query have synonym entries in the thesaurus, and if they do, adds the synonyms to the query.</td>
</tr>
<tr>
<td>Automatically use corrected query suggestion (did you mean)</td>
<td>When selected, automatically corrects misspelled keywords in the query before sending the query to the index server.</td>
</tr>
<tr>
<td>Open emails with Microsoft Outlook</td>
<td>When selected, allows users to open email search results with Microsoft Outlook.</td>
</tr>
</tbody>
</table>

5. Click **Apply** to make changes effective.

8.7.9.7 .NET Interface Editor - Advanced Menu

This section gathers topics related to administrative procedures that are not regularly performed by a Coveo Platform administrator such as the association of one or more security providers to a Coveo .NET Front-End search interface.

8.7.9.7.1 What Are Alternate URI Rules?

Alternate URIs are addresses used to open documents from a source or application different from the one used for indexing.

**Example:** You can open Microsoft Exchange emails in a Web interface instead of the native Microsoft Outlook mail client.
8.7.9.7.2 Creating Alternate URI Rules for a .NET Search Interface

Alternate URIs are addresses used to open documents from a source or application different from the one used for indexing.

**Example:** You can open Microsoft Exchange emails in a Web interface instead of the native Microsoft Outlook mail client.

To create an alternate URI rule

1. Access the Coveo .NET Front-End Interface Editor.
2. Access the **Search Interfaces** tab.
3. In the **Current Interface** drop-down box, select the search interface for which you want to create an alternate URI rule.
4. Select **Advanced > Alternate Uris**.
5. Click **Add New**.

6. Edit the appropriate parameters described in the following table.

<table>
<thead>
<tr>
<th>Section</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Description</td>
<td>Indicates the purpose of the rule.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong> Open emails in a Web application.</td>
</tr>
<tr>
<td>Uri Pattern</td>
<td>Indicates the addresses affected by this rule (i.e. replaced by the alternate address). Use wildcards if necessary.</td>
</tr>
<tr>
<td>Replacement</td>
<td>Indicates the address used to open the documents. Select <strong>Enabled by default</strong> to apply the rule by default and <strong>Mandatory</strong> to make the rule compulsory.</td>
</tr>
</tbody>
</table>
7. Click OK.

8.7.9.7.3 Adding Security Providers to a .NET Search Interface

A Coveo .NET Front-End search interface can get and pass to the Coveo Back-End server the identity of the user performing a query so that only documents this user has permissions to see are returned in search results.

Sometimes a user needs to search using multiple user identities at the same time. You can allow a user to do this by associating one or more security providers to the .NET search interface. When one or more security providers are added to a .NET search interface, a lock icon appears in the top-right corner of the .NET search interface to allow the user to access a login form where they can enter additional credentials.

**Example:** A user is logged in with their Windows account and accesses the All Content .NET search interface in a Coveo Web access point. The user queries return only documents that their Active Directory account has permissions to see, not Claims-enabled SharePoint documents that the user should legitimately see.

You add the SharePoint Claims security provider to the .NET search interface. The user can log in to provide their SharePoint Claims credentials. When this is done, both his Active directory and Claims identities are passed to the Back-End server so that Claims-enabled SharePoint documents can also be returned in the search results.

**Notes:**

- You must first configure the security provider in the Administration Tool.

- The login form requires a secured .NET search interface access (HTTPS). When the search interface is accessed via HTTP, the login form includes a message indicating that HTTPS must be used.

  **Coveo .NET Front-End 12.0.295+ (August 2013)** The username and password are sent to the server via the SSL connection and an authorization token is stored in an end-user browser cookie (not the username and password). By default the cookie expires when the user closes the browser but to avoid having to log in for each new browser session, selecting the Keep me logged in check box makes the cookie valid for one month.

- When adding a Claims SharePoint security provider, ensure that the Coveo web service is installed on a SharePoint front-end server to allow the login to work.
To add security providers to the .NET search interface

1. Access the Coveo .NET Front-End Interface Editor.
2. Access the Search Interfaces tab.
4. Click Add New.
5. In the Edit Security Provider page:
   - In the Title box, enter a descriptive name for the security provider. This name appears in the lock icon pop up window and in the login form.
   - In the Security Provider drop-down list, select the appropriate security provider.
     
     **Example:** For Claims-based SharePoint server, select your Claims security provider.

     **Note:** The Security Provider lists only security providers of types supporting the login feature. By default only Active Directory is available. Ensure that one or more valid security providers of type supporting the login are configured in CES.

   - Select the Automatically Ask to Login check box when you want to automatically display the login form in the search interface when a user starts a search session.
     
     It is generally recommended to select this check box to systematically propose to users to provide their additional credentials so that all search results to which they are entitled are returned. When the check box is cleared, the user must know and remember to manually click the lock icon on the search interface top bar to open the login form and enter his credentials.

     **Notes:** The Login or Cancel user actions are persisted on a per user per browser basis. As long as a user is using the same browser session, he will not have to log in again or cancel an automatic form. For security reason, only an authorization token provided by CES is stored in a browser cookie, not the entered Username and Password.

   - Click OK.
6. It is recommended to configure IIS to force an HTTPS search interface connection or automatically redirect HTTP to HTTPS to prevent users from seeing the login form error message "To login, your browser must
connect via HTTPS (secured HTTP connection).) and having to manually change the search interface URL from http:// to https:// (see IIS7: HOW TO force a website to use SSL? and HTTP Redirects <httpRedirect>).

What’s Next?

Go back to the search interface, refresh the page, and then login with your additional identity to validate that you can now find documents secured with this additional identity.

8.7.9.7.4 Configuring a Custom Scope With the .NET Interface Editor

**CES 7.0.5556– (June 2013)**

*IMPORTANT: CES 7.0.5639+ (July 2013)* The Coveo .NET Front-End custom scope feature is replaced by the Back-End search scope feature (see "What Are Search Scopes?" on page 360).

Each Coveo .NET Front-End search interface has a specific scope (see "Configuring the Scope of a .NET Search Interface" on page 597). You can also define one or more custom scopes that are defined using either a filter expression or by connecting to a remote index. A custom scope can also optionally exclude the index from the local Coveo instance.

While a normal scope is transparent to the end-user, a custom scope is accessible from the .NET search Interface Search In facet that appears when one or more custom scopes are available.

**Example:** In your Los Angeles head office, you can create custom scopes to exclusively search in the Boston or Paris remote indexes within your organization. End-users can select the desired scope when needed from the Search In facet.

To configure a custom scope with the .NET Interface Editor

1. Access the Coveo .NET Front-End Interface Editor.
2. Select the Search Interfaces tab.
3. In the Current Interface drop-down box, select the search interface for which you want to configure the custom scope.
4. Select the Advanced menu.
5. In the navigation panel on the left, select Custom Scopes.
6. Do one of the following action:
   a. To create a new custom scope, click Add New next to Custom Search Scopes.
   OR
   b. To modify a custom scope, click its name.
7. Under Edit Custom Scope:
a. In the **Title** box:
   i. Enter a descriptive name meaningful to end-users as they will view it as an option in the **Search In** facet.
   ii. Click the button next to the box to open a dialog box where you can enter the label translated for the other supported languages.

b. Enter a specific filter **Expression** in the form of a query.

   **Note:** The filter expression defines the custom scope but also applies to remote indexes if included.

c. Select the **Exclude local server from search** check box when you want to exclude the local index from the scope and only query remote indexes.

8. When remote indexes have already been defined in the Administration Tool for the current Coveo instance (see "Adding or Modifying Remote Indexes" on page 355), you can also add one or more remote indexes to the custom scope:

   a. Next to **Remote Indexes**, click **Add**.

   b. From the **Name** drop-down list, select the appropriate remote index.

   c. In the **Filter Expression** box, enter a filter expression to add to every query sent to the remote index.

   d. In the **Time to execute (sec)** box, enter the maximum time to wait for the query results from the remote index. A warning message appears in the search interface when the time out is reached. The default value is 0, in which case the search interface waits indefinitely.

   **Note:** When the remote Coveo instance is down, local search results are presented immediately without waiting for remote results.

9. Click **OK**.
8.7.9.8 Enabling the Question Mark Wildcard Behavior in a .NET Search Interface

The question mark character (?) is ignored by default (interpreted as space character) in a Coveo .NET Front-End search interface when included in a query. You can however configure the question mark to behave as a wildcard character when used in a query.

The main reason why the question mark wildcard behavior is disabled by default is to allow end-users to search for question phrases.

**Example:** An end-user performs a natural language search for a document title that is a question, and he includes the question mark at the end of the phrase:

```
what are wildcards?
```

By default, the question mark wildcard behavior is disabled, the ? character is ignored and the index returns documents containing the wildcards term.

When the question mark wildcard behavior is enabled, the ? character is interpreted as a wildcard and the index only returns documents containing terms that match wildcards plus one (any) character at the end like wildcards1 or wildcardss, thus excluding documents containing wildcards, and most probably excluding documents that would be useful to the end-user.

**Coveo .NET Front-End 12.0.57+ (November 2012)** When the benefits of the question mark used as a wildcard in queries overcome the inconvenient mentioned above in your context, you can enable the question mark wildcard behavior.

To enable the question mark wildcard behavior in a .NET search interface

1. Using an administrator account, connect to your Coveo Front-End server.
2. Locate the folder of the skin used by the search interface in which you want to enable the question mark wildcard behavior.
3. Using a text editor:
   a. Open the CoveoSearch.ascx file.
   b. Add the following code to the end of the file:

   ```
   <script runat="server">
   protected override void OnInit(EventArgs p_Args)
   {
   base.OnInit(p_Args);
   SetupSearchBuilder += MySetupSearchBuilder;
   }
   void MySetupSearchBuilder(object p_Sender, SetupSearchBuilderEventArgs p_Args)
   {
   p_Args.Builder.UseQuestionMarkAsWildcards = true;
   }
   </script>
   ```
   c. Save the file.
4. Repeat the procedure for each search interface skin and each Front-End server for which you want to enable the question mark wildcard behavior.

8.7.10 .NET Interface Editor - Audiences Tab

Coveo .NET Front-End audiences are groups and users that you can associate to .NET search interfaces when added to a hub to control access to each .NET search interface. In the Audiences tab, you can create, modify, and delete audiences.

8.7.10.1 What Is an Audience?

In the Coveo .NET Front-End, an audience is a group of people corresponding to a category of users. An audience is made of Active Directory groups and users (see "Adding an Audience With the .NET Interface Editor" on page 636).

You can associate audiences independently for each .NET search interface when you add them to a .NET search hub. When accessing a .NET search hub, a user only sees the user interfaces associated with audiences for which he or she is a member (see "Adding Search Interfaces to a Search Hub With the .NET Interface Editor" on page 544).

Example: You can create an audience grouping all the employees from the marketing department. You create a .NET search interface to meet the search needs of this department. When you add the .NET search interface to the .NET search hub, you assign this audience to the .NET search interface so that only marketing department users can see this interface.

8.7.10.2 Adding an Audience With the .NET Interface Editor

A Coveo .NET Front-End audience is made of Active Directory groups and users. The purpose of audiences is to control access to .NET search interfaces within a .NET search hub (see "Adding Search Interfaces to a Search Hub With the .NET Interface Editor" on page 544).

To add an audience With the .NET Interface Editor

1. Access the Coveo .NET Front-End Interface Editor.
2. Select the Audiences tab.
3. Click Add New.
4. In the **Name** box, enter a descriptive name for the new audience.

This name will appear in the page where you can add search interfaces to a search hub (see "Adding Search Interfaces to a Search Hub With the .NET Interface Editor" on page 544).

5. Beside **Groups** or **Users**, respectively for each group or user that you want to include in the audience:
   a. In the lower box, enter the name of a valid Active Directory group/user for the current domain.

   **Note:** You cannot add a group or user from a domain other than the one in which the Coveo server resides.

   b. Click Add.

   The group or user appears in the upper box when it is authenticated. An error message appears at the top of the page when the name is not recognized.

6. To delete a group or a user, select the group or user name in the appropriate upper box, and then click **Delete**.

7. Click **OK**.

8.7.11 .NET Interface Editor - Miscellaneous Tab

In the Coveo .NET Front-End Interface Editor **Miscellaneous** tab, you can configure the following aspects:
Custom File Types

Used to associate an icon to a custom file type retrieved by the Coveo Platform. The icon appears next to search results of the custom file type, making it easier to identify by end-users (see "Adding Custom File Types With the .NET Interface Editor" on page 638).

Per URI Settings

Used to display different .NET search interfaces for a group of addresses even if their corresponding pages cannot be edited (see "Adding a Per URI Setting With the .NET Interface Editor" on page 639).

Example: In SharePoint, the pages corresponding to several sites can share the same .aspx file. Therefore, modifications to this file are applied to all sites. However, it is possible to display different .NET search interfaces in those pages by using per URI settings (see "Adding a Per URI Setting With the .NET Interface Editor" on page 639).

Language

Used to select the language of the .NET Interface Editor user interface (English or French) and the available languages for the .NET search interfaces (see "Configuring the Available .NET Search Interface Languages" on page 640).

### 8.7.11.1 Adding Custom File Types With the .NET Interface Editor

The out-of-the-box Coveo .NET Front-End search interfaces come with icons for common file types. The appropriate icon appears in front of a search result to help users more easily identify the file type for each result. When a file type is unknown, a default icon is used.

When you want to change the icon appearing for search results of a specific file type, you can define a custom file type and associate the desired icon.

**Note:** Custom file types must first be defined in the Administration Tool (see "Modifying How CES Handles a Document Type" on page 477).

To add a custom file type with the .NET Interface Editor

1. Access the Coveo .NET Front-End Interface Editor.
2. Select the **Miscellaneous** tab, and then select **Custom File Types** in the navigation panel on the left.
3. Click **Add New**.
4. Under **Edit Custom File Type**: 

   - [www.coveo.com](http://www.coveo.com)
8.7.11.1 Adding a Custom File Type

In Name, enter a descriptive name for the file type.

In Value of @sysfiletype field, enter the extension of the appropriate file type.

Example: For a Microsoft Word file you would enter docx.

In the Icon Uri box, enter the path for the icon file. You can specify the full path in the [site_address]/[path]/[image_file] form or the relative path from where the search interface page is stored.

Examples:
Absolute path: http://mysite.com/images/icon-people.png
Relative path: /Coveo/Skins/MyInterface/icon-people.png

Click OK.

5. Under Custom File Types, you can delete custom formats by selecting them and clicking Delete.

8.7.11.2 Adding a Per URI Setting With the .NET Interface Editor

Per URI settings allow to display different Coveo .NET Front-End search interfaces for a group of addresses even if their corresponding pages cannot be edited.

Example: In Microsoft SharePoint, pages corresponding to several sites can share the same .aspx file, and modifications to this file are applied to all sites. However, it is possible to display different .NET search interfaces within those pages by using per URI settings.

To add a per URI setting with the .NET Interface Editor

1. Access the Coveo .NET Front-End Interface Editor.
2. Access the Per Uri Settings page (Miscellaneous > Per Uri Settings).
3. Click Add New.
4. Under Edit Per Uri Settings:
a. In **Uri Pattern**, enter the addresses of the pages to replace, using wildcards characters (*, ?) when necessary.

b. In **Uri of the search page**, enter the address of the appropriate search page.

c. In the **Name of Interface** drop-down list, select the search interface to display.

d. Click **OK**.

**What's Next?**

Add a .NET search interface to your hub and select the **Overridable by Per Uri settings or query string arguments** option (see "Adding Search Interfaces to a Search Hub With the .NET Interface Editor" on page 544.

8.7.11.3 Configuring the Available .NET Search Interface Languages

The Coveo .NET Front-End out-of-the-box search interfaces are available in several languages. You can configure the culture of a .NET search hub or of .NET search interfaces to appear in the appropriate language (see "Configuring the Culture of a Search Hub With the .NET Interface Editor" on page 550 and "Configuring the Culture of a .NET Search Interface" on page 596).

You can also add or remove available languages in which all .NET search interfaces can appear.

**Examples:**

- You created a custom English .NET search interface from an out-of-the-box one and you translated the new .NET search interface text elements only to French. Therefore, you do not want the Spanish, German, Dutch, and Portuguese versions to be available as the translation is incomplete for these languages.

- You add a Greek .NET search interface that is not available out-of-the-box. Therefore, you add Greek as an available .NET search interface language and provide Greek translations for all .NET search interface text elements by editing the Coveo multi-language XML interface string files.

To configure the available .NET search interface languages

1. Access the Coveo .NET Front-End Interface Editor.

2. Select the **Miscellaneous** tab, and then select **Language** in the navigation panel on the left.

3. Under **Search Interface:**
To remove one or more available languages:

a. Select the check box of one or more languages that you want to remove.

b. Click Delete.

c. Click Yes at the confirmation prompt.

To add a language:

a. Click Add New.

b. In the drop-down list that appears under Add Language, select the language that you want to add in the list of languages that CES can detect, and then click OK.

c. To add the translation for this new language for a given label, click the button appearing at the end of the parameter box to open the dialog box in which you can enter the translation for each available language.
d. To add the translations for all the search interface strings for this new language, using a text editor:

i. In the [.NET_Front-End_Path]\Web\Strings\ folder, open the CNLStrings.xml and SearchStrings.xml files.

ii. For each string name, add a line that encloses the corresponding translation for the new language.

Example: To add a Swedish (SV) translation for the Cancel button, add a line after those for the other existing languages:

```xml
<string name="Cancel" language="de">Abbrechen</string>
<string name="Cancel" language="en">Cancel</string>
<string name="Cancel" language="es">Cancelar</string>
<string name="Cancel" language="fr">Annuler</string>
<string name="Cancel" language="nl">Annuleren</string>
<string name="Cancel" language="pt">Cancelar</string>
<string name="Cancel" language="sv">Avbryta</string>
```

iii. Save the files.

8.7.11.4 Changing the .NET Interface Editor Language

The Coveo .NET Front-End Interface Editor is available in English and French. You can manually change the language in which the user interface of the .NET Interface Editor appears.

To change the .NET Interface Editor language

1. Access the Coveo .NET Front-End Interface Editor.

2. Select the Miscellaneous tab, and then select Language in the navigation panel on the left.
3. In the drop-down list under **Interface Editor**, select **English** or **French**.

![Interface Editor](image)

### 8.7.11.5 Importing CES 6.x .NET Search Interface Settings

At the end of the CES 7 software installation process, you can choose to create the index using your CES 6.x configuration rather than creating a new index from scratch (see "Creating a New Index or Importing an Existing CES 6 Index Configuration" on page 40). If you made this choice, your CES 6.x customized .NET search interface settings were also copied from the CES 6.x index configuration file (`[Index_Path]\config\config.txt`) to the same file for the CES 7 instance.

With the Coveo .Net Front-End 12 however, the customized .NET search interface settings are no longer stored in the index configuration file but rather in XML files located in the ` [.NET_Front-End_Path]\Web\Coveo\Skins` folder. At this point you do not see your customized .NET search interface settings in the .NET Interface Editor. To recover your custom .NET search hubs and .NET search interfaces, a last step is needed to complete the import process.

**Note:** The import settings process transfers all the configuration changes that you can do in the .NET Interface Editor except those related to CSS styles that are done in the **Search Interfaces > Settings** menu. You can modify the styles from the .NET Interface Editor (see "Modifying .NET Search Interface CSS Styles" on page 618). Modifications to skin .ascx files made by a developer are not imported either and must be migrated manually.

To import CES 6.x .NET search interface settings

1. Access the Coveo .NET Front-End Interface Editor.
2. Select **Miscellaneous > Import Settings**.
3. In the **Import Settings From CES 6.5** page:

   When you chose to create the index using your CES 6.x configuration and customized search interface settings were available, the elements to import are presented and the **Import** button is enabled.
Example: In the following case, customized settings for one hub and 3 search interfaces were imported from a CES 6.5 instance.

Note: The page can also list missing skins referenced from search interfaces, or missing search hubs. In these cases, manually copy the missing files from the CES 6.x server to the Coveo .NET Front-End server before importing the settings.

a. Click Import.

b. At the confirmation prompt:
   * Click Yes only when you understand that importing the settings would overwrite customized settings done locally for search hubs and/or search interfaces with the same name as those to import.

   An import confirmation message appears at the top of the page.

   In the [.NET_Front-End_Path]\Web\Coveo\Skins folder, XML files are created for each element with customized settings.

   Note: The XML files contain only the customized parameters, not all the parameters for the customized elements. The standard parameters are determined in the Coveo DLLs.

   OR

   * Click No to cancel the import.

8.7.12 .NET Interface Editor - Deployment Tab

The features of the .NET Interface Editor Deployment tab allow you to easily replicate the settings of all your .NET search interfaces from one Coveo .NET Front-End server to one or more other Front-End servers. These features allow to implement a Front-End staging process within a Coveo instance or between Coveo instances.

8.7.12.1 Planning Your Front-End Staging Process

In the Coveo Platform 7, all the files associated with search interfaces are contained in the [.NET_Front-End_Path]\Web\Coveo\Skins folder on each Front-End server. Each Front-End server contains its copy of the search interface folders.
Example: The files for the My Computer search interface are stored in the C:\Program Files\Coveo .NET Front-End 12\Web\Coveo\Skins\My Computer folder.

You can implement a Front-End staging process in an environment where you have two or more Coveo Front-End servers. You use one of the Front-End servers as the staging server where you customize and test search interfaces without affecting the other Front-End servers. When you are ready to synchronize the other Front-End servers, you use the Deployment tab of the Interface Editor to easily replicate the search interfaces from the source staging Front-End server to one or more target production Front-End servers. You can deploy search interfaces within a Coveo instance or between Coveo instances.

Important: For the Coveo Platform 7 Beta 1 only, to be able to successfully use the search interface settings deployment, you must run the http://localhost:[Port_number]/?ExportSettings=1 URL once on each Front-End server to generate local XML files in the [.NET_Front-End_Path]\Web\Coveo\Skins\ folder.

To plan your Front-End staging process

1. Identify one of your Coveo Front-End servers as the staging Front-End server.

2. When your Coveo Front-End servers are organized in a network load-balancing (NLB) cluster, pull the staging Front-End server out of the NLB cluster (see "Configuring Coveo Servers in a Network Load-Balancing Cluster" on page 98).

3. On the staging Front-End server:
   a. Using the Interface Editor, customize and test one or more search interfaces.
   b. Create the list of target Front-End servers to which you want to replicate search interface settings (see "Managing the List of Target Front-End Servers" on page 645).
   c. Push the settings of the search interfaces from the staging Front-End server to one or more production Front-End servers (see "Deploying Search Interface Settings" on page 647).

4. For NLB configurations, bring back the staging Front-End server into the NLB cluster.

8.7.12.2 Managing the List of Target Front-End Servers

You can use the features of the Deployment tab in the Interface Editor to replicate all the search interface settings from one Coveo Front-End server to one or more target Front-End servers. This feature is useful to easily implement a Front-End staging process (see "Planning Your Front-End Staging Process" on page 644).

Before deploying interfaces from a source Front-End server to target Front-End servers, on the source Front-End server, you must create the list of Front-End servers to which you want to push search interface settings.

To manage the list of target Front-End servers

1. On the source Coveo Front-End server, the one you identified as the staging Front-End server, access the Interface Editor (see "Opening the .NET Interface Editor" on page 537).

2. In the Interface Editor, select the Deployment tab.

3. In the Deployment tab:
To add a new target Front-End server to the list:

a. Click **Add**.

b. On the new table row:
   
i. In the **URL** column, enter the URL of the target Coveo Front-End server in the `http://[Front-End_Server]:[Port_number]` format.

   ii. In the **User Account** column, enter the user name for the account used to connect to the target server. Enter the name in the `domain\username` format, and then enter the corresponding password.

   **Important:** The specified user must:
   
   - Be an Active Directory user.
   - Be a member of either the Administrator or Search Interface Designer administration role (see "About Administration Roles" on page 406). In the case of a Front-End server connected to a remote index, the user administration role must be defined in the Master server of the remote Coveo instance.
   - Have read/write access to the `C:\Program Files\Coveo .NET Front-End 12\folder` on the Front-End server.

   iii. Click the check mark icon (✔) to complete the server addition.

The local server attempts to connect to the target server and reports the connection results in the **Status** column as described in the following table.

<table>
<thead>
<tr>
<th>Status</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>![Up-to-Date]</td>
<td>The search interfaces files on the target Front-End server are an exact replica of the ones on the source server.</td>
</tr>
<tr>
<td>Status</td>
<td>Description</td>
</tr>
<tr>
<td>----------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>[Date]</td>
<td>The search interfaces files on the target Front-End server are NOT an exact replica of the ones on the source server. The date indicates the last modification date for the search interface files on the target server.</td>
</tr>
<tr>
<td>Unavailable</td>
<td>The connection to the target server failed. A tooltip describing the error appears when you leave the pointer over the status.</td>
</tr>
</tbody>
</table>

**Note:** Ensure that firewalls on both servers allow the communication on the specified port.

- To edit the parameters for a target Front-End server:
  - Click the pencil icon (📝) at the end of the row for the server that you want to edit.
  - Edit the **URL** and **User Account** columns, and then click the check mark icon (✔).

- To eliminate a target Front-End server from the list:
  - a. In the table, select the check box at the beginning of the row for the server that you want to eliminate.
  - b. Click **Delete**.
  - c. When prompted to confirm the deletion, click **Yes**.

OR

  - a. In the table, click the delete icon (❌) at the end of the row for the server that you want to eliminate.
  - b. When prompted to confirm the deletion, click **Yes**.

**What's Next?**

When your search interfaces are ready on the staging Front-End server, replicate the search interface settings from the source Front-End server to one or more target Front-End servers (see "Deploying Search Interface Settings" on page 647).

### 8.7.12.3 Deploying Search Interface Settings

In a Front-End staging process, you can customize and test search interface settings on a staging Front-End server (see "Planning Your Front-End Staging Process" on page 644). Once the settings are validated, you can easily replicate the settings for all the search interfaces of the staging Front-End server to one or more target Front-End servers. This is done using the features of the **Deployment** tab in the Interface Editor, where you can also build your list of target Front-End servers (see "Managing the List of Target Front-End Servers" on page 645). The deployment integrally copies the content of the `.NET_Front-End_Path\Web\Coveo\Skins` folder.

**Note:** The deployment of the search interface settings is done without target Front-End server interruption. A Front-End server keeps search interface settings in cache memory. The target server cache memory update happens only after all search interface files have been synchronized and is triggered when the next query is received. The end-user who sent this query is the only one experiencing a longer response time due to cache memory loading.
Important: The Coveo Professional Services or your internal developers can create custom assemblies for your Coveo Front-Ends to implement personalized features. When new or updated custom assemblies are used on your staging Front-End server, you must manually copy them from the staging Front-End server to the target Front-End servers before deploying the search interface settings. The custom assembly DLLs reside in the [.NET_Front-End_Path]\bin folder.

To deploy the search interface settings

1. On the source Coveo Front-End server, the one you identified as the staging Front-End server, access the Interface Editor (see "Opening the .NET Interface Editor" on page 537).

2. In the Interface Editor, select the Deployment tab.

3. In the Deployment tab:
   a. In the list of target Front-End servers, select the check box for one or more servers to which you want to push the search interface settings.
   b. Click Deploy.
   c. When prompted to confirm to overwrite settings of front-ends, click Yes.

   Note: On each target Front-End server, prior to overwrite the search interface settings, a local backup folder containing the original search interface files ([.NET_Front-End_Path]\Web\Coveo\Backup\[yyyy-mm-dd_hhmmss]) is created. You can always roll back to this version by manually copying the content of the backup folder into the [.NET_Front-End_Path]\Web\Coveo\Skins folder.

   d. In the Deploy Settings on Front-Ends page, validate that the Succeeded! status appears, and then click Return to list.

www.coveo.com
The List of front-ends servers page shows that the target server has an **Up-to-Date** status.

8.8 On-Premises Usage Analytics Module

**Deprecated** The on-premises Usage Analytics module is no longer maintained by Coveo. Rather consider using the Coveo Usage Analytics cloud service to monitor on-premises search usage (see Coveo Cloud Usage Analytics).

The Usage Analytics module provides information that helps administrators optimize their Coveo .NET search implementation by analyzing the paths users follow while searching and navigating in the results. By tracking and understanding user behavior, the administrator can better determine the user search requirements, assess performance of the system, and optimize their search results – ultimately increasing adoption of the .NET search solution.

The on-premises Usage Analytics database automatically tracks all user actions performed in the Coveo .NET Front-End search interfaces, including result click-through, faceted navigation, and the use of the different user interface functions. The actions are saved in the database along with user information, search session data, and the opened documents on which the action was taken.

The administrator uses the Usage Analytics user interface to view and analyze the logged information. The **Analytics** user interface offers numerous filters to help find precise search usage information.
Note: The Analytics tab appears at the top of the default web interface only after the Usage Analytics module has been deployed and only when the user has Coveo administrator rights. End-users do not see the Analytics tab.

Steps for using the Usage Analytics module

1. Deploy the Usage Analytics module

   You need to setup the database that will collect the Usage Analytics data, enable the Usage Analytics module, and then connect it to the database (see "Deploying the On-Premises Usage Analytics Module" on page 651).

   If you experience problems, see "Troubleshooting and Handling Usage Analytics Module Errors" on page 665.

2. Learn how to use the Analytics user interface

   The Analytics user interface contains numerous filters allowing you to quickly and easily review the Usage Analytics data (see "Analytics User Interface Elements" on page 659 and "Refining Usage Analytics Results" on page 660).
3. Exploit the Usage Analytics data

The Usage Analytics data being collected in a database, you can develop your own queries and even customize the data that is collected (see "Usage Analytics Database Content" on page 667 and "Customizing the Collected Usage Analytics Data" on page 675).

8.8.1 Deploying the On-Premises Usage Analytics Module

**Deprecated** The on-premises Usage Analytics module is no longer maintained by Coveo. Rather consider using the Coveo Usage Analytics cloud service to monitor on-premises search usage (see Coveo Cloud Usage Analytics).

The Usage Analytics module components are included when you set up a Coveo .NET Front-End server but the Usage Analytics features are turned off by default.

The Usage Analytics module also requires to connect to a Microsoft SQL database where it will log search and navigation actions. You can use an existing Microsoft SQL Server or create a new SQL Server instance. The Coveo .NET Front-End and the Microsoft SQL database can be installed on the same server or on different servers. You can deploy the Usage Analytics module on a single Coveo server configuration or on a multiple Coveo Back-End and Front-End server topology.

In summary, the deployment process consists in creating a dedicated Microsoft SQL database, setting the permissions to the database, and on each Coveo Front-End server, activate and configure the Usage Analytics module to connect to this database.

Usage Analytics module requirements:


  **Note:** Coveo .NET Front-End 12.0.252+ (June 2013) Support for SQL Server 2012.

- You need Coveo and Microsoft SQL Server administrator rights to perform the following procedure.

- Microsoft Silverlight support in the browser used to view the Analytics user interface.

  **Note:** The Coveo new breed of search usage analytics offering is in the cloud. You are encouraged to use the Coveo Cloud Usage Analytics service to monitor on-premises search usage (see Coveo Cloud Usage Analytics).

To deploy the Usage Analytics module

1. Choose an existing Microsoft SQL Server or install a new instance where the Usage Analytics database will be created.

2. Note the name of the Microsoft SQL Server instance.

3. On the Coveo Front-End server, find the name of the user that runs the Coveo site in IIS (see "Finding the Name of the User that Runs a Process in IIS" on page 78).

4. On the Microsoft SQL Server, create a new empty Usage Analytics database using the default name CoveoAnalytics (see "Creating a Database in Microsoft SQL Server" on page 88).
Note: You can use a different database name, but you will need to specify this name in the Web.config file later in this procedure. Also, before running the database creation script, you will need to edit the first line of the database creation script to replace the default database name with the name you selected.

5. Run the appropriate database creation script distributed in the [.NET_Front-End_Path]\Web\Analytics\Scripts\Creation folder (see “Running a Script in Microsoft SQL Server” on page 92).

Example: With CES 7.0, run the CREATE_CES_ANALYTICS_DB_V7-1.SQL script.

Important: Use the creation script only the first time that you start using the Usage Analytics module. Running the creation scripts permanently erases any existing Usage Analytics data as it creates blank Usage Analytics database tables.

If you are installing a new version of CES and deployed the Usage Analytics module for an earlier version, you may need to perform migration tasks for the Usage Analytics database (see “Updating the Usage Analytics Database Format” on page 655).

6. In Microsoft SQL Server Management Studio, set read and write access rights to the database for the user that runs the CES service:

a. In the Object Explorer pane, expand the Security folder, right-click on Logins, and then select New Login in the contextual menu.

b. In the Login - New dialog box, create a login for the user identified in step 3, and then click OK.

Example: When CES and Microsoft SQL run on the same server and the identified user is NetworkServices, create a NT AUTHORITY\NETWORK SERVICE login.

Example: When CES and Microsoft SQL run on different servers and the identified user is NetworkServices, create a [CESserverdomain]\[CESservername]$ login, where you replace [CESserverdomain] and [CESservername] by the appropriate names.

c. Back in the Object Explorer pane, expand Security and Logins, right-click on the newly created login
name, and then select Properties in the contextual menu.

d. In the Login Properties dialog box, select the CoveoAnalytics database as well as the db_datareader and db_datawriter check boxes as shown below.

7. On the Microsoft SQL Server, in the SQL Server Configuration Manager, ensure that the protocol used by CES to communicate with the SQL database is activated (as shown in the Microsoft SQL 2008 example in the following figure). Restart the SQL server after making changes.
8. When CES and Microsoft SQL run on different servers, ensure that the firewall of the Microsoft SQL Server allows communication from the Coveo server (typically on port 1433).

9. On each Coveo Front-End server, edit the Web.config file to activate the Usage Analytics module and configure to which SQL Server it connects:

**Notes:**

- **Coveo .NET Front-End 12.0.664+ (March 2014)** These settings can be made automatically during the first time setup.
- It is recommended to make a backup of the web.config file before editing it.
- Repeat the following steps for all search servers in your Coveo deployments including integrations such as in SharePoint or a website.

a. Using a text editor, open the Coveo Front-End web.config file.

**Example:**

- **On a Coveo Front-End server:** [.NET_Front-End_Path]\Web\Web.config.
- In the case of a SharePoint integration, the web.config file is at the root of each SharePoint virtual servers (usually located in C:\inetpub\wwwroot\wss\VirtualDirectories\{PortNumber}).

b. In the file, after the <coveoEnterpriseSearch> tag, locate the following line:

```xml
<analytics enabled="false" connectionString="Data Source=yourServerName;Initial Catalog=CoveoAnalytics;Integrated Security=SSPI;"/>
```

c. Edit the line as follows:

i. Change enabled="false" to enabled="true" to activate the Usage Analytics data collection.

ii. Replace yourServerName by the name of the Microsoft SQL Server that will host the Usage Analytics...
database (noted in step 2) to set the database connection string (connectionString=).

Example: When CES and Microsoft SQL run on the same server, replace yourServerName by localhost or by \<yourServerName>\<SQLInstance> for a specific SQL Server instance like MyMachine\SQLExpress or .\SQLExpress.

When CES and Microsoft SQL run on different servers, replace yourServerName by a string of the form SQLservername.yourcompany.com or by the IP address of the Coveo server.


iii. If you used a database name other than the default name when you created the database, replace CoveoAnalytics by the name you used.

d. Save the Web.config file.

The Usage Analytics module immediately starts to collect search usage information to the database and the Analytics user interface tab appears in the default Coveo .NET search interface (for a Coveo administrator only).

Important: If you have more than one Coveo Front-End server, repeat the editing of the Web.config file on each Front-End server to also collect search usage from these servers.

Tip: You can customize the Usage Analytics data collection behavior by configuring the Web.config file (see "Customizing the Collected Usage Analytics Data" on page 675).

10. On the Coveo Front-End server, test the Usage Analytics module:

   a. Using a Coveo administrator account, open the default Coveo search page (Windows taskbar Start > All Programs > Coveo Enterprise Search 7 > Default Search Interface).

   b. Perform a few queries to ensure that some data is sent to the Usage Analytics database.

      If an error message appears, the connection or the permissions to the database may not be set properly (see "Troubleshooting and Handling Usage Analytics Module Errors" on page 665).

   c. In the default .NET search interface, click the Analytics tab to open the user interface.

   d. If Microsoft Silverlight is not yet installed on your server, click the Install Microsoft Silverlight icon that appears to install it.

   e. Verify that the Analytics user interface presents the queries that you performed.

8.8.2 Updating the Usage Analytics Database Format

The format of the Microsoft SQL database used to collect the Usage Analytics data may change when you upgrade from one Coveo Platform version to another. When your Coveo implementation takes advantage of the Usage Analytics module features, in the Coveo migration process, you therefore need to update the Usage Analytics database to the latest format.
To update the Usage Analytics database format

1. Referring to the following table, select the migration scripts appropriate for your migration. The scripts files are distributed in the [.NET_Front-End_Path]\Web\Analytics\Scripts\Migration\ folder.

<table>
<thead>
<tr>
<th>Script file</th>
<th>CES version</th>
</tr>
</thead>
<tbody>
<tr>
<td>MIGRATE_CES_ANALYTICS_DB_FROM_V7_TO_V7-1.SQL</td>
<td>7.0</td>
</tr>
<tr>
<td>MIGRATE_CES_ANALYTICS_DB_FROM_V6_TO_V7.SQL</td>
<td>6.5.4616+</td>
</tr>
<tr>
<td>MIGRATE_CES_ANALYTICS_DB_FROM_V5_TO_V6.SQL</td>
<td>6.5.4332+</td>
</tr>
<tr>
<td>MIGRATE_CES_ANALYTICS_DB_FROM_V4_TO_V5.SQL</td>
<td>6.5 up to release 4280</td>
</tr>
<tr>
<td>MIGRATE_CES_ANALYTICS_DB_FROM_V3_TO_V4.SQL</td>
<td></td>
</tr>
<tr>
<td>MIGRATE_CES_ANALYTICS_DB_FROM_V2_TO_V3.SQL</td>
<td>6.2</td>
</tr>
<tr>
<td>Note: You also need to run ReviseAnalytics method (see the corresponding Step).</td>
<td></td>
</tr>
<tr>
<td>MIGRATE_CES_ANALYTICS_DB_FROM_V1_TO_V2.SQL</td>
<td>6.1</td>
</tr>
</tbody>
</table>

**Important:** Pay attention to not use the creation script also available in the Creation folder. Running the creation script permanently erases any existing Usage Analytics data as it creates blank Usage Analytics database tables.

**Example:** You are migrating from CES version 6.5 build 4332 in which the Usage Analytics module database is in version 5. You need to migrate the Usage Analytics database to version 7-1. To do so, you must successively run the following scripts:

- MIGRATE_CES_ANALYTICS_DB_FROM_V5_TO_V6.SQL
- MIGRATE_CES_ANALYTICS_DB_FROM_V6_TO_V7.SQL
- MIGRATE_CES_ANALYTICS_DB_FROM_V7_TO_V7-1.SQL

2. On the Coveo server, copy the appropriate script file from the [.NET_Front-End Path]\Web\Analytics\Scripts folder.

**Note:** The script uses the Usage Analytics database default name (CoveoAnalytics). If your implementation of the Usage Analytics database uses a different name, edit the first line of the script to replace the default database name with the name of your database.

3. On the Microsoft SQL Server:
   a. Paste the script file to a temporary folder of your choice.
   b. Start Microsoft SQL Server Management Studio (on the Windows taskbar, select Start > All Programs >
Microsoft SQL Server 2008 > SQL Server Management Studio).

4. In Microsoft SQL Server Management Studio:
   a. On the menu, select File > Open > File.
   b. In the Open File dialog box, browse for the script file that you pasted, and then click OK.
   c. On the SQL Editor toolbar, select the appropriate database (CoveoAnalytics by default), and then click Execute to run the script.

A message appears at the bottom of the Microsoft SQL Server Management Studio window to indicate that the execution of the script completed successfully.

A migration log is also added in the Version table of the Usage Analytics database.

<table>
<thead>
<tr>
<th>versionId</th>
<th>versionCreatedDate</th>
<th>versionNumber</th>
<th>versionData</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>2010-08-23 15:33:08.200</td>
<td>2</td>
<td>0</td>
</tr>
<tr>
<td>2</td>
<td>2010-08-23 15:33:47.217</td>
<td>3</td>
<td>1</td>
</tr>
<tr>
<td>3</td>
<td>2010-10-26 09:59:33.920</td>
<td>4</td>
<td>0</td>
</tr>
</tbody>
</table>

5. When you migrate the Usage Analytics database from version 2 to version 3, immediately after running the
MIGRATE_CES_ANALYTICS_DB_FROM_V2_TO_V3.SQL script, you also need to invoke the \texttt{ReviseAnalytics} Usage Analytics web service method to populate the newly created Keywords and ActionKeywords tables with your existing Usage Analytics data:

a. Using a browser, on the Coveo Master server, access the Usage Analytics web service page with the following URL:

\texttt{http://localhost:8080/Coveo/Analytics/Analytics.asmx?op=ReviseAnalytics}

b. In the page that appears, click \texttt{Invoke}.

The \texttt{ReviseAnalytics} method performs the required operations in the background.

8.8.3 Opening the Analytics User Interface

You can review Coveo .NET Front-End search interface events recorded by the Usage Analytics module from the Analytics user interface.

Notes:

- The Analytics user interface tab appears in the default .NET search interface only for a Coveo administrator.
- You can also access the Analytics user interface using the following URL format: \texttt{http://[ServerName]:[port]/Analytics}

\textbf{Example:} \texttt{http://MyCoveoFrontEndServer:8080/Analytics}

To open the Analytics user interface

1. Using a Coveo administrator account, on a Coveo Front-End server, open the default .NET search interface (on the Windows taskbar select \texttt{Start > All Program > Coveo Enterprise Search 7 > Default Search Interface}).
2. On the .NET search interface toolbar, click **Analytics**.

### 8.8.4 Analytics User Interface Elements

The **Analytics** user interface is divided in four sections as shown in the following example and legend.

**Popular**

The available options for the **Top <Popular>** list that appears in section 3 and shows the corresponding most frequent elements found in the Usage Analytics database (for example, as shown in the previous figure, selecting **Users** displays the **Top Users** list).

**Timeline graph**

The timeline graph shows the number of queries recorded as a function of time for the current filter selection.

**Top <Popular> list**

The **Top <Popular>** list presents the found elements for the current selection in the **Popular** list, starting with the most frequent elements. You can click an element in the list to refine the results to that element and drill down further using other criteria that appear in the list title bar (see "Refining Usage Analytics Results" on page 660).

**Filter selectors**

The filter selectors allow you to refine the **Top <Popular>** list content (see "Refining Usage Analytics Results" on page 660). The timeline graph is also updated to show the number of filtered queries. The filter selector box is shaded in green when the filter is active. The following table presents the available filters.
<table>
<thead>
<tr>
<th>Filter type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface Filter</td>
<td>Lists the .NET search interfaces from which queries were performed. Select the check box of one or more .NET search interfaces to update the Top &lt;Popular&gt; list and the timeline graph with queries entered only in the selected .NET search interfaces. This filter is useful to evaluate the adoption of a .NET search interface.</td>
</tr>
<tr>
<td>Misc Filter</td>
<td>Presents a selection of the following special filters:</td>
</tr>
<tr>
<td></td>
<td><strong>No results returned</strong>  Lists only queries for which no results were found. This filter is useful to help identify the gap between the available content and what users are looking for.</td>
</tr>
<tr>
<td></td>
<td><strong>At least one result was opened</strong> Lists only queries for which the user clicked to open at least one result.</td>
</tr>
<tr>
<td></td>
<td><strong>User switched to next page</strong> Lists only queries for which the user opened at least one other search results page in the .NET search interface. This filter is useful to identify content that users are looking for and do not find within the first results page.</td>
</tr>
<tr>
<td></td>
<td><strong>User changed the query</strong> Lists only queries that were modified by the user within a query session. This filter is useful to identify original queries with which user probably did not find what they were looking for.</td>
</tr>
<tr>
<td>Query Filter</td>
<td>Presents a box to type and search one or more specific queries so that it can be added as a custom filter. When more than one custom filters are selected, the underlying query uses an OR logical operator between the expressions.</td>
</tr>
<tr>
<td>Keyword Filter</td>
<td>Presents a box to type and search one or more specific keywords so that it can be added as a custom filter. When more than one custom filter is selected, the underlying query uses an OR operator between the keywords.</td>
</tr>
<tr>
<td>User/Group Filter</td>
<td>Presents a box to type and search one or more specific users or groups of users so that they can be added as a custom filter.                                                                                                           This filter is useful to help evaluate the adoption of the search tool by a user or by a group of users.</td>
</tr>
<tr>
<td>SuperUser Access Filter</td>
<td>Lists the super user accesses granted to the current user. This filter only appears for a user that was granted super user access.                                                                                                        This filter is useful to easily track all actions that you performed using privilege super user tokens.</td>
</tr>
<tr>
<td>Query Source Filter</td>
<td>Lists the access points from which listed queries were performed. This filter is useful to determine from which access points users perform searches.</td>
</tr>
</tbody>
</table>

8.8.5 Refining Usage Analytics Results

In the **Analytics** user interface, you can refine the results using the following methods:
Refining Usage Analytics results for a specific date interval

In the Analytics user interface, you can easily filter results for a date range using the timeline graph.

1. Open the Analytics user interface (see “Opening the Analytics User Interface” on page 658).
2. In the lower part of the timeline graph that shows the number of queries for the complete date range available from the Usage Analytics database, click and drag the date range start and end markers to set the desired date range.

The upper part of the timeline graph and the Top <Popular> list are updated to show only the newly selected date range.

Refining Usage Analytics results using the filters

The Analytics user interface includes filter selectors to help you refine the presented results (see “Analytics User Interface Elements” on page 659). You can use one, or a combination of filters, to narrow the results presented in the Top <Popular> list and in the timeline graph.

1. Open the Analytics user interface (see “Opening the Analytics User Interface” on page 658).
2. In the Popular list, select the desired element for which you want to see Top <Popular> results.
3. To use a filter selector, click its box to expand it.
4. When the filter selector contains predefined check boxes (as shown in the following figure):
a. Click one or more check boxes to refine the **Top <Popular>** list to the corresponding selection.

The filter selector box turns green to indicate that a filter is active.

b. Click **Check all** or **Uncheck all** when you want to respectively select or clear all available check boxes.

5. When a filter selector contains a box (as shown in the following figure):

![Filter Selector]

a. In the box, start typing the text with which you want to create a custom filter.

As you type, text completion and a list below the box automatically appear, matching available elements from the Usage Analytics database.

b. Select one of the available choices.

c. Click ![Add](+) on the right of the box to add the element as a custom filter.

The custom filter appears as a check box above the box.

d. Select the newly created check box to activate the custom filter.

e. To eliminate a custom filter from the filter selector, click ![Remove](−) on the right of the custom filter.

**Refining Usage Analytics results using the Top <Popular> list**

You can click a **Top <Popular>** list element to see details about the selected element.
1. Open the Analytics user interface (see "Opening the Analytics User Interface" on page 658).

2. In the Popular list, select the desired elements for which you want to see the Top <Popular> results (for example Search Interfaces).

3. In the Top <Popular> list:
   a. Click a result for which you want to see details.

   The Top <Popular> list is refined to this selection. The element you clicked appears on the title bar of the Top <Popular> list together with a series of tabs.

   b. On the Top <Popular> list title bar, click the desired tab to see the corresponding details.

   c. Click [Go Back] to clear the previous Top <Popular> list selection.

   ![Diagram of Search Interface Detail]

   1. A result clicked in the top results list for which details are shown.
   2. A selected tab, showing corresponding details.
   3. Click [Go Back] to clear the previous top results list selection.

8.8.6 Evaluating the .NET Search Solution Adoption

You can use the Analytics user interface to evaluate who uses the Coveo .NET search solution, from what access point, and using which .NET search interface. The following procedures provide simple examples of how you can do this. Use one or combinations of the following procedures.

Finding who uses the search solution

1. Open the Analytics user interface (see "Opening the Analytics User Interface" on page 658).

2. In the Popular list, click Users.

3. Review the Top Users list to see the most frequent users.

4. In the time line graph, change the date range selection to see if the most frequent users change as a function of time.
5. To narrow the search solution adoption evaluation to a specific group of users:
   a. In the filer selector area on the left, click **User/Group Filter** to expand the filter box.
   b. In the box, start to type the name of the desired group, and then select the desired group in the list that automatically appears.

   The Top Users list and the timeline graph are updated to only show queries and users from this group.

6. Repeat the previous step for other or combinations of other groups.

Finding which .NET search interfaces are used

1. Open the Analytics user interface (see "Opening the Analytics User Interface" on page 658).
2. In the Popular list, click **Search Interfaces**.
3. Review the Search Interface Detail list to see the most frequently used .NET search interfaces.
4. In the time line graph, change the date range selection to see if the most frequently used .NET search interface changes as a function of time.
5. To narrow the results to one or a few specific .NET search interfaces:
   - In the Search Interface Detail list, click a .NET search interface.
   OR
   a. In the filter selector area on the left, click **Interface Filter** to expand the filter box.
   b. Select the check box of one or more .NET search interfaces.

   The Search Interface Detail list and the timeline graph are updated to only show information from this or these .NET search interfaces.

Finding from which access point searches are performed

1. Open the Analytics user interface (see "Opening the Analytics User Interface" on page 658).
2. In the filter selector area on the left, click **Query Source Filter** to open the filter box.
3. Select the check box of one or more access point to narrow the Top <Popular> list content to this selection.
4. Use the Popular list to update the Top <Popular> list and see the search usage from the selected access point.
8.8.7 Identifying the Gap Between the Available and the Searched Content

You can use the Analytics user interface to identify the content that users are looking for and that is missing, not found, or harder to find. The following procedures provide simple examples of how you can do this.

Identifying missing content

1. Open the Analytics user interface (see "Opening the Analytics User Interface" on page 658).
2. In the Popular list, click Queries or Keywords.
3. In the filter selector area on the left, click Misc Filter to expand the filter box.
4. Select the No results returned check box.
5. Review the Top <Popular> list to see the most frequent queries or keywords for which no results were returned.
   - You can forward a relevant summary of missing content to the people who can improve existing or create new content to fill the knowledge gap.
   - You can also use this information to feed the Coveo thesaurus to increase the number of successful queries.

Identifying harder to find content

1. Open the Analytics user interface (see "Opening the Analytics User Interface" on page 658).
2. In the Popular list, click Queries or Keywords.
3. In the filter selector area on the left, click Misc Filter to expand the filter box.
4. Select the User switched to next page or the User changed the query or both check boxes.
5. Review the Top <Popular> list to see the most frequent queries or keywords for which the user worked harder.
   - You can forward a relevant summary of hard to find content to the people who can improve existing or create new related content.
   - You can also use this information to feed the Coveo thesaurus to increase the number of successful queries.

8.8.8 Troubleshooting and Handling Usage Analytics Module Errors

- When CES and Microsoft SQL run on different servers, ensure that the firewall of the Microsoft SQL Server allows communication from the Coveo server (typically on port 1433).

- Verify that the Microsoft SQL Server identified in the Web.config file exists, is running, and that the user that runs the Coveo website in IIS on the Coveo Front-End servers has the read and write permissions to the database (see "Deploying the On-Premises Usage Analytics Module" on page 651).

- Most Usage Analytics module errors are linked to problems with the connection to the Microsoft SQL Server. In the Web.config file, make appropriate changes to the connectionString parameter (refer to the following website for details: http://www.connectionstrings.com/sql-server-2008).

- In Sql Server Configuration Manager, ensure that the protocol used by CES to communicate with the SQL
database is activated (see the example for Microsoft SQL 2008 in the following figure).

![Sql Server Configuration Manager](image)

8.8.8.1 Usage Analytics error messages

By default, the Usage Analytics module displays errors below the search box in the Coveo .NET search interface. These Usage Analytics module errors only appear for a Coveo administrator, not for end-users.

**Note:** You can configure the Usage Analytics module to log errors (see "Logging Usage Analytics Module Errors" on page 676).

You may encounter the following Usage Analytics module errors:

- **Analytics Error:** A network-related or instance-specific error occurred while establishing a connection to SQL Server. The server was not found or was not accessible. Verify that the instance name is correct and that SQL Server is configured to allow remote connections. (provider: Named Pipes Provider, error: 40 - Could not open a connection to SQL Server)

  - Possible causes:
    - The SQL server is not running or not accessible.
  - Possible solutions:
    - Ensure that the connection string and the permissions are configured correctly (see "Deploying the On-Premises Usage Analytics Module" on page 651).
    - In **Sql Server Configuration Manager**, ensure that the Named Pipes protocol used by CES to
communicate with the SQL database is activated.

- When you use Microsoft SQL Server Express 2012, consider the instructions in Enable remote connections for SQL Server Express 2012.

8.8.9 Usage Analytics Database Content

You may want to take advantage of data collected by the Usage Analytics module by directly querying the Usage Analytics database. This section presents detailed information on the content of the Usage Analytics database.

This topic contains the following sections:

- "Usage Analytics database schema" on page 667
- "Content of Usage Analytics database tables" on page 668
- "Relations between tables in the Usage Analytics database" on page 672
- "Logged actions" on page 673
- "Logged values" on page 674

8.8.9.1 Usage Analytics database schema

The following schema presents all the tables and the relations between the tables of the Usage Analytics database.
8.8.9.2 Content of Usage Analytics database tables

The following table describes the content of each Usage Analytics database table.
## Table

<table>
<thead>
<tr>
<th>Table</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Users</strong></td>
<td>Represents a user that accesses one of the .NET search interfaces monitored by the Usage Analytics module.</td>
</tr>
<tr>
<td></td>
<td>- userId: (PK) The unique identifier of the user.</td>
</tr>
<tr>
<td></td>
<td>- userCreatedDate: The date at which the user was created.</td>
</tr>
<tr>
<td></td>
<td>- userName: The full name of the user.</td>
</tr>
<tr>
<td><strong>UserMetadata</strong></td>
<td>Represents metadata related to a specific user. This entity is used to store additional information (see “Customizing the Collected Usage Analytics Data” on page 675).</td>
</tr>
<tr>
<td></td>
<td>- usermetadataId: (PK) The unique identifier of the user metadata.</td>
</tr>
<tr>
<td></td>
<td>- usermetadataName: The name of the metadata.</td>
</tr>
<tr>
<td></td>
<td>- usermetadataValue: The value of the metadata.</td>
</tr>
<tr>
<td><strong>Sessions</strong></td>
<td>Represents a sequence of interactions between a user and a .NET search interface. Looking at the sequence of actions in a session allows administrators to determine if a search session was a success or not.</td>
</tr>
<tr>
<td></td>
<td>- sessionId: (PK) The unique identifier of the session.</td>
</tr>
<tr>
<td></td>
<td>- sessionCreatedDate: The date at which the session was created.</td>
</tr>
<tr>
<td></td>
<td>- sessionGuid: The globally unique identifier (GUID) of the session. This value is required by the .NET search interface as there is a strong distinction between the search user interface and the mechanism responsible for writing in the database.</td>
</tr>
<tr>
<td></td>
<td>- userId: (FK) The user related to the session.</td>
</tr>
<tr>
<td><strong>SessionMetadata</strong></td>
<td>Represents the metadata related to a specific session. This entity is used to store additional information (see “Customizing the Collected Usage Analytics Data” on page 675).</td>
</tr>
<tr>
<td></td>
<td>- sessionmetadataId: (PK) The unique identifier of the session metadata.</td>
</tr>
<tr>
<td></td>
<td>- sessionmetadataName: The name of the metadata.</td>
</tr>
<tr>
<td></td>
<td>- sessionmetadataValue: The value of the metadata.</td>
</tr>
<tr>
<td><strong>SearchInterfaces</strong></td>
<td>Represents the .NET search interfaces on which data is collected.</td>
</tr>
<tr>
<td></td>
<td>- searchInterfaceId: (PK) The unique identifier of the .NET search interface.</td>
</tr>
<tr>
<td></td>
<td>- searchInterfaceCreatedDate: The date at which the .NET search interface was created.</td>
</tr>
<tr>
<td></td>
<td>- searchInterfaceName: The name of the .NET search interface.</td>
</tr>
<tr>
<td>Table</td>
<td>Description</td>
</tr>
<tr>
<td>-------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Actions</td>
<td>Represents any action that can be performed on a .NET search interface. This table is the central part of the Usage Analytics database design.</td>
</tr>
<tr>
<td></td>
<td>* actionId: (PK) The unique identifier of the action.</td>
</tr>
<tr>
<td></td>
<td>* actionCreatedDate: The date the action was performed.</td>
</tr>
<tr>
<td></td>
<td>* actionGuid: The globally unique identifier (GUID) of the action. This value is required by the .NET search interface as there is a strong distinction between the search UI and the mechanism responsible for writing in the database.</td>
</tr>
<tr>
<td></td>
<td>* actionType: The type of the action (see &quot;Logged actions&quot; on page 673).</td>
</tr>
<tr>
<td></td>
<td>* actionOutputType: The type of output the action has generated (ex.: web, RSS, xml, etc.).</td>
</tr>
<tr>
<td></td>
<td>* sessionId: (FK) The session in which the action was performed.</td>
</tr>
<tr>
<td></td>
<td>* searchInterfaceId: (FK) The .NET search interface the action was performed on.</td>
</tr>
<tr>
<td></td>
<td>* searchHubId: (FK) The search hub the action was performed from.</td>
</tr>
<tr>
<td></td>
<td>* parentActionId: (FK) The action ID of the parent of the action.</td>
</tr>
<tr>
<td></td>
<td>* actionResponseTime: The time required to perform the action.</td>
</tr>
<tr>
<td></td>
<td>* rootActionId: (FK) The action ID of the root of the action.</td>
</tr>
<tr>
<td></td>
<td>* queryId: (FK) The query ID related to this action.</td>
</tr>
<tr>
<td>ActionValues</td>
<td>Represents the various values related to an action.</td>
</tr>
<tr>
<td></td>
<td>* actionId: (PK) (FK) The action ID the action value is related to.</td>
</tr>
<tr>
<td></td>
<td>* actionValueName: (PK) The name of the action value.</td>
</tr>
<tr>
<td></td>
<td>* actionValueStringValue: The string representation of the action value.</td>
</tr>
<tr>
<td></td>
<td>* actionValueIntegerValue: The integer representation of the action value.</td>
</tr>
<tr>
<td></td>
<td>* actionValueDoubleValue: The double representation of the action value.</td>
</tr>
<tr>
<td></td>
<td>* actionValueDateTimeValue: The date and time representation of the action value.</td>
</tr>
<tr>
<td>Queries</td>
<td>Represents the various queries entered by users.</td>
</tr>
<tr>
<td></td>
<td>* queryId: (FK) The unique identifier for the query.</td>
</tr>
<tr>
<td></td>
<td>* queryExpression: The expression of the query.</td>
</tr>
<tr>
<td>SearchHubs</td>
<td>Represents the various search hubs.</td>
</tr>
<tr>
<td></td>
<td>* searchHubId: (PK) The unique identifier of the search hub.</td>
</tr>
<tr>
<td></td>
<td>* searchHubCreatedDate: The date at which the search hub was created.</td>
</tr>
<tr>
<td></td>
<td>* searchHubName: The name of the search hub.</td>
</tr>
<tr>
<td>Results</td>
<td>Represents the results on which an action is performed. This entity is a bridge between an action and documents.</td>
</tr>
<tr>
<td></td>
<td>* actionId: (PK) (FK) The action that targets the result.</td>
</tr>
<tr>
<td></td>
<td>* documentId: (PK) (FK) The document targeted by the result.</td>
</tr>
<tr>
<td></td>
<td>* resultListIndex: The order in which the result was displayed.</td>
</tr>
<tr>
<td></td>
<td>* resultIsTopResult: Boolean indicating when the result is a Top Result.</td>
</tr>
<tr>
<td>Table</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Documents</td>
<td>Represents documents that are available for the search. Basically, it holds information to find this document in the index.</td>
</tr>
<tr>
<td></td>
<td>- documentId: (PK) The unique identifier of the document.</td>
</tr>
<tr>
<td></td>
<td>- documentCreatedDate: The date at which the document was created.</td>
</tr>
<tr>
<td></td>
<td>- documentAggregatedMirrorId: The ID of the aggregated mirror the document came from.</td>
</tr>
<tr>
<td></td>
<td>- documentPhysicalIndexName: The name of the physical index the document came from.</td>
</tr>
<tr>
<td></td>
<td>- collectionId: (FK) The ID of the collection the document came from.</td>
</tr>
<tr>
<td></td>
<td>- sourceId: (FK) The ID of the source the document came from.</td>
</tr>
<tr>
<td></td>
<td>- documentUrl: The URL of the document.</td>
</tr>
<tr>
<td>DocumentMetadata</td>
<td>Represents metadata related to a specific document. This identity is used to store additional information (see &quot;Customizing the Collected Usage Analytics Data&quot; on page 675).</td>
</tr>
<tr>
<td></td>
<td>- documentmetadataId: (PK) The unique identifier of this document metadata.</td>
</tr>
<tr>
<td></td>
<td>- documentmetadataIndexedDate: The date this document was indexed.</td>
</tr>
<tr>
<td></td>
<td>- documentmetadataName: The name of the metadata.</td>
</tr>
<tr>
<td></td>
<td>- documentmetadataValue: The value of the metadata.</td>
</tr>
<tr>
<td></td>
<td>- documentId: (FK) The document related to this metadata.</td>
</tr>
<tr>
<td>Collections</td>
<td>Represents collections from which sources come from.</td>
</tr>
<tr>
<td></td>
<td>- collectionId: (PK) The unique identifier of this collection (@syscollection from CES).</td>
</tr>
<tr>
<td></td>
<td>- collectionIndexedDate: The date at which the collection name was indexed.</td>
</tr>
<tr>
<td></td>
<td>- collectionName: The name of the collection.</td>
</tr>
<tr>
<td>Sources</td>
<td>Represents sources from which documents come from.</td>
</tr>
<tr>
<td></td>
<td>- sourceId: (PK) The unique identifier of this source (@syssource from CES).</td>
</tr>
<tr>
<td></td>
<td>- sourceIndexedDate: The date the source name was indexed.</td>
</tr>
<tr>
<td></td>
<td>- sourceName: The name of the source.</td>
</tr>
<tr>
<td>ActionKeywords</td>
<td>Represents the various keywords related to an action.</td>
</tr>
<tr>
<td></td>
<td>- actionId: (FK) The ID of the action related to this keyword.</td>
</tr>
<tr>
<td></td>
<td>- keywordId: (FK) The unique identifier of the keyword</td>
</tr>
<tr>
<td>Keywords</td>
<td>Represents the various query keywords.</td>
</tr>
<tr>
<td></td>
<td>- keywordId: (FK) The unique identifier of the keyword</td>
</tr>
<tr>
<td></td>
<td>- keywordValue: The keyword itself.</td>
</tr>
</tbody>
</table>
Table | Description
--- | ---
**Versions (Internal Coveo Table)** | Represents the version of this database. This is a utility table used by CES to determine if the database is up-to-date. - `versionId`: (PK) The unique identifier of the version. - `versionCreatedDate`: The date the version was installed. - `versionNumber`: The main version number (for example "4" in 4.0). - `versionData`: The data version number (for example "0" in 4.0).

8.8.9.3 Relations between tables in the Usage Analytics database

The following table provides a description of the relations between Usage Analytics database tables.

<table>
<thead>
<tr>
<th>Table Relation</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>User – UserMetadata</td>
<td>Users can have zero or more metadata. By default, CES does not store metadata on users. This table is filled by custom data (see &quot;Customizing the Collected Usage Analytics Data&quot; on page 675).</td>
</tr>
<tr>
<td>User – Session</td>
<td>A session must be initiated by a user. If a .NET search interface allows anonymous connections, then the anonymous user initiates all the sessions on that .NET search interface.</td>
</tr>
<tr>
<td>Session – SessionMetadata</td>
<td>Sessions can have zero or more metadata. By default, CES does not store metadata on sessions. This table is filled by custom data (see &quot;Customizing the Collected Usage Analytics Data&quot; on page 675).</td>
</tr>
<tr>
<td>Session – Action</td>
<td>An action must be performed on a specific session. This relation allows administrators to link every action performed to a specific user.</td>
</tr>
<tr>
<td>SearchHub – Action</td>
<td>An action can be performed on a specific search hub. This allows administrators to track statistics on specific search hubs.</td>
</tr>
<tr>
<td>Search Interface – Action</td>
<td>An action must be performed on a specific .NET search interface. This allows administrators to track statistics on specific .NET search interfaces.</td>
</tr>
<tr>
<td>Parent Action – Action</td>
<td>A series of actions can be performed to complete a search session. This relation allows administrators to follow the search path of a user through the .NET search interface.</td>
</tr>
<tr>
<td>Root Action – Action</td>
<td>Actions are based on a root action. A root action is the first action of a search path of a user through the .NET search interface.</td>
</tr>
<tr>
<td>Action – ActionValue</td>
<td>An action contains one or more action values (see &quot;Logged values&quot; on page 674).</td>
</tr>
<tr>
<td>Action – Result</td>
<td>An action contains zero or more search results depending on the action type.</td>
</tr>
</tbody>
</table>
### Table Relation | Description
--- | ---
Document – Result | A document is linked to one or more search results across the actions.
Document – DocumentMetadata | Documents can have zero or more metadata. By default, CES does not store metadata on documents. This table is filled by custom data (see "Customizing the Collected Usage Analytics Data" on page 675).
Source – Document | Documents must be located in a source.
Collection–Document | Documents must be located in a collection.
Action – ActionKeyword | An action can have zero or more action keywords depending on the action type.
Keyword – ActionKeyword | A keyword is linked to one or more action keyword across the actions.
Query – Action | A query is linked to one or more action.

### 8.8.9.4 Logged actions

The following table lists the action types logged by the Usage Analytics module. You can overwrite these actions in ASP.net (see "Customizing the Collected Usage Analytics Data" on page 675).

<table>
<thead>
<tr>
<th>Logged action type</th>
<th>Logged action name</th>
</tr>
</thead>
<tbody>
<tr>
<td>CHANGE_INTERFACE</td>
<td>&quot;ChangeInterface&quot;</td>
</tr>
<tr>
<td>CLEAR_REFINE_BY_FIELD</td>
<td>&quot;ClearRefineByField&quot;</td>
</tr>
<tr>
<td>DID_YOU_MEAN</td>
<td>&quot;DidYouMean&quot;</td>
</tr>
<tr>
<td>EXPAND_QUERY</td>
<td>&quot;ExpandQuery&quot;</td>
</tr>
<tr>
<td>EXPORT_TO_EXCEL</td>
<td>&quot;ExportToExcel&quot;</td>
</tr>
<tr>
<td>FILTER_REFINE_BY_FIELD</td>
<td>&quot;FilterRefineByField&quot;</td>
</tr>
<tr>
<td>MANUAL_RATING</td>
<td>&quot;ManualRating&quot;</td>
</tr>
<tr>
<td>OPEN_CACHED_VERSION</td>
<td>&quot;OpenCachedVersion&quot;</td>
</tr>
<tr>
<td>OPEN_DOCUMENT</td>
<td>&quot;OpenDocument&quot;</td>
</tr>
<tr>
<td>PAGE_CHANGE</td>
<td>&quot;PageChange&quot;</td>
</tr>
<tr>
<td>Logged action type</td>
<td>Logged action name</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>------------------------------</td>
</tr>
<tr>
<td>PERFORM_SEARCH</td>
<td>&quot;PerformSearch&quot;</td>
</tr>
<tr>
<td>RATE_THIS_SEARCH</td>
<td>&quot;RateThisSearch&quot;</td>
</tr>
<tr>
<td>REFINE_BY_CLUSTER</td>
<td>&quot;RefineByCluster&quot;</td>
</tr>
<tr>
<td>REFINE_BY_FIELD</td>
<td>&quot;RefineByField&quot;</td>
</tr>
<tr>
<td>REFINE_BY_SCOPE</td>
<td>&quot;RefineByScope&quot;</td>
</tr>
<tr>
<td>REMOVE_REFINE_BY_CLUSTER</td>
<td>&quot;RemoveRefineByCluster&quot;</td>
</tr>
<tr>
<td>REMOVE_REFINE_BY_FIELD</td>
<td>&quot;RemoveRefineByField&quot;</td>
</tr>
<tr>
<td>REMOVE_REFINE_BY_SCOPE</td>
<td>&quot;RemoveRefineByScope&quot;</td>
</tr>
<tr>
<td>RSS_LINK</td>
<td>&quot;RSSLink&quot;</td>
</tr>
<tr>
<td>SEARCH_WITHIN_RESULTS</td>
<td>&quot;SearchWithinResults&quot;</td>
</tr>
<tr>
<td>SHOW_DETAILS</td>
<td>&quot;ShowDetails&quot;</td>
</tr>
<tr>
<td>SHOW_IN_DETAIL_VIEW</td>
<td>&quot;ShowInDetailView&quot;</td>
</tr>
<tr>
<td>SORT_BY_FIELD</td>
<td>&quot;SortByField&quot;</td>
</tr>
</tbody>
</table>

8.8.9.5 Logged values

The following table lists the value types logged by the Usage Analytics module.

<table>
<thead>
<tr>
<th>Logged value type</th>
<th>Logged value name</th>
</tr>
</thead>
<tbody>
<tr>
<td>CLUSTER_NAME</td>
<td>&quot;ClusterName&quot;</td>
</tr>
<tr>
<td>DOCUMENT_SCORE</td>
<td>&quot;DocumentScore&quot;</td>
</tr>
<tr>
<td>FACET_TYPE_NAME</td>
<td>&quot;FacetTypeName&quot;</td>
</tr>
<tr>
<td>FIELD_LOOKUP</td>
<td>&quot;FieldLookup&quot;</td>
</tr>
<tr>
<td>FIELD_NAME</td>
<td>&quot;FieldName&quot;</td>
</tr>
<tr>
<td>FIELD_VALUE</td>
<td>&quot;FieldValue&quot;</td>
</tr>
<tr>
<td>OUTPUT_TYPE</td>
<td>&quot;OutputType&quot;</td>
</tr>
<tr>
<td>PREVIOUS_INTERFACE</td>
<td>&quot;PreviousInterface&quot;</td>
</tr>
</tbody>
</table>
You can customize the data that the Usage Analytics module collects.

8.8.10.1 Adding custom data

The `DocumentFields` parameter needs to be added in the `Web.config` file (edited in "Deploying the On-Premises Usage Analytics Module" on page 651) to be able to log document metadata into the Usage Analytics database. The `DocumentFields` value is a comma-separated list of custom fields.

Note: It is recommended to make a backup of the `web.config` file before editing it.
8.8.10.2 Modifying actions before they are saved into the database

The following C# code is an example that adds information to an action before it is saved. The following example, added to the ASPX page, changes the values for UserId, SiteId, and ActionValueMedata (current date and time) before they are saved into the SQL database.

```csharp
<%@ Import Namespace="Coveo.CES.Web.Search.Analytics" %>
<script language="c#" runat="server">
    protected override void OnLoad(EventArgs p_Args)
    {
        this.ReportCustomActionData +=
            delegate(object sender, AnalyticsActionEventArgs args)
        {
            args.ActionData.UserMetadata.Add("UserId", "test1234567890");
            args.ActionData.SessionMetadata.Add("SiteId", "site #987654321");
            args.ActionData.Values.Add(new ActionValueData("myDate", DateTime.Now));
        };
    }
</script>
```

8.8.10.3 Creating custom actions

This example is similar to the one shown in "Modifying actions before they are saved into the database" on page 676 except that it adds values on custom actions based on your own events that are not in the predefined list of logged actions (see "Usage Analytics Database Content" on page 667).

```csharp
using Coveo.CES.Web.Search.Analytics;
var values = new List<ActionValueData>() { new ActionValueData("myActionValue", "valueToLog")};
AnalyticsLogging.LogAction(SearchObject, "myAction", ActionValueNames.OutputTypeValues.WEB, values, null);
```

8.8.11 Logging Usage Analytics Module Errors

If you need to collect Usage Analytics module errors, you can create a log of these errors by adding a parameter to the Web.config file on each Coveo Front-End server.

To log Usage Analytics module errors

1. On the Coveo Front-End server, using a text editor, open the [.NET_Front-End_Path]\Web\Web.config file.

   **Note:** It is recommended to make a backup of the web.config file before editing it.

2. In the file, after the <coveoEnterpriseSearch> tag, locate the following line:

   ```xml
   <analytics enabled="true" connectionString="Data Source=yourServerName;Initial Catalog=CoveoAnalytics;Integrated Security=SSPI;"/>
   ```

3. Add the logFolder="[log_folder_path]" parameter to the line, changing [log_folder_path] to the desired path.
Example:

```xml
<analytics enabled="true" connectionString="Data Source=yourServerName;Initial Catalog=CoveoAnalytics;Integrated Security=SSPI;" logFolder="C:\AnalyticsLogFolder"/>
```


5. When your Coveo server topology includes more than one Front-End server, repeat this procedure for each Front-End server.

### 8.8.12 Deactivating the Usage Analytics Module

You can deactivate the Usage Analytics module by editing the `Web.config` file on each Coveo Front-End server. Deactivating the Usage Analytics module turns off the collection of Coveo search and navigation user interface usage to the database and eliminates the Analytics tab from the default .NET search interface.

**Note:** It is recommended to make a backup of the `web.config` file before editing it.

To deactivate the Usage Analytics module:

1. On the Coveo Front-End server, open the `[.NET_Front-End_Path]\Web\Web.config` file with a text editor.

2. Under `<coveoEnterpriseSearch>`, locate the following line:

   ```xml
   <analytics enabled="false" connectionString="Data Source=yourServerName;Initial Catalog=CoveoAnalytics;Integrated Security=SSPI;"/>
   ```

3. Replace `enabled="true"` by `enabled="false"` to deactivate the Usage Analytics module.


   The Usage Analytics module immediately stops to collect search usage data and the Analytics tab is no longer available in the default .NET search interfaces on this Front-End server.

5. When your Coveo topology includes more than one Front-End server, repeat this procedure on each Front-End server.

### 8.8.13 Usage Analytics Cloud Service

Coveo offers two options to record and review usage of your Coveo search interfaces:

- Cloud Usage Analytics service hosted in the cloud (see Coveo Cloud Usage Analytics).

  OR

- Legacy on-premises Usage Analytics module that uses a local database (see "On-Premises Usage Analytics Module" on page 649).

The Coveo Usage Analytics cloud service uses a dedicated Coveo cloud Organization to record search events performed by the users in your various Coveo search interfaces.

**Note:** If you do not have access to the Coveo Usage Analytics cloud service, contact your Coveo Sales representative.
Once you have access to your Coveo Usage Analytics cloud Organization, you will get an authorization token that will be used by the search interface to securely authenticate itself to the Organization when it sends search interface events.

An administrator can configure a Coveo .NET Front-End server to send search interface events to the Coveo Usage Analytics cloud Organization when the first time setup is performed (see Coveo .NET Front-End First Time Setup).

Similarly, a developer can configure a Coveo JavaScript Search interface to send search interface events to the Coveo Usage Analytics cloud service (see Analytics Component).

8.9 OCR Module

The Optical Character Recognition (OCR) module allows you to index text content from files such as scanned documents stored in image or PDF files.

**Supported document formats**

- .tiff, .tiff-fx, .pcx, .dcx, .bmp, .jpeg, .png, .max, .gif, .pnm, and .pdf

**Supported languages**

- 120 non-Asian languages
- 21 languages with spell checking dictionaries for improved detection (Brazilian, Catalan, Czech, Danish, Dutch, English, Esperanto, Finnish, French, German, Greek, Hungarian, Italian, Norwegian, Polish, Portuguese, Russian, Slovenian, Spanish, Swedish, Turkish)

It is recommended to separate the source files requiring OCR conversion from those that do not. This ensures the highest level of performance and conversion quality. You can do this by moving files in different file system folders or through the use of source filters (see "Adding or Modifying Source Filters" on page 295).
Notes:

- The OCR module is optional. You need to purchase it to receive the license allowing you to install and activate the module.
- **CES 7.0.5989+ (October 2013)** The OCR module can run as a 64-bit process.
- By default, to minimize useless processing of a large number of small files that do not contain text, such as icons, the OCR module does not process small files.

Depending on your CES version:

- **CES 7.0.6607+ (April 2014)** Small files are indexed by reference.
- **CES 7.0.6547– (March 2014)** Small files are not indexed.

- The default OCR module configuration is a compromise between conversion completeness and performances and can prevent indexing some content in a document or even entire documents. Consider adapting the configuration to your needs (see "Tuning the OCR Module" on page 683).

- OCR licensing (CPUs, cores, and threads)

  OCR licensing works on a CPU basis. Each licensed OCR module allows you to pass OCR through one CPU, with a number of threads equal to the number of cores in that CPU. This is due to the third party component at the core of the module and implies that some further measures need to be taken for you to maximize your OCR use.

  - Consider the number of CPUs on your server. Do you want to use all CPUs for OCR? Purchase one OCR module per CPU you want to use.
  - Provide Coveo with the total number of cores so that they can prepare the licensing accordingly. OCR licensing only includes one thread by default.

You can set the number of OCR threads for the local or remote converters (see "Configuring a Remote Converter" on page 458).

Note that if you look at the processes in the Task Manager while OCR is running, even with a single licensed OCR, you may occasionally see more than one OCR process. That is due to the fact that a process is spawned for each individual page of a multi-page document.

**CES 7.0.6684+ (May 2014)** You can see the number of concurrent OCR converters authorize by your CES license by reviewing the Audio Video Restrictions parameter value from the License page (see "What Information Is Displayed in the License Page?" on page 525).

Deployment overview

1. Download and install the OCR module on your Coveo server (see "Installing the Optical Character Recognition Module" on page 69).
2. Let CES know where to find the OCR converter (see "Adding an OCR Open Converter" on page 680).
3. Create a new document type set (see "Creating a Document Type Set" on page 477).
4. Link the OCR open converter to appropriate document types (see "Associating the OCR Open Converter to..."
5. Assign the document type set to sources containing documents to be converted with the OCR module (see "Modifying the Document Type Set Used by a Source" on page 481).

**Tip:** When you have a large number of documents to process using OCR, it is good practice to:

a. Starting indexing a source containing only a small representative sample of documents.

b. Validate that all documents and all their desired content has been indexed as expected.

c. If not make adjustments (see "Tuning the OCR Module" on page 683).

d. Once satisfied, index all documents.

6. Rebuild the sources.

8.9.1 Adding an OCR Open Converter

After running the Optical Character Recognition (OCR) installer (see "Installing the Optical Character Recognition Module" on page 69), you must add an open converter for the OCR module.

To add an OCR open converter

1. Using an administrator account, connect to the Coveo Master server.

2. If it does not already exist, create the [Index_Path]\Scripts folder. The default folder is C:\CES7\Scripts.

3. Copy the [CES_Path]\OCR Module\OCRConversion7.js file to the [Index_Path]\Scripts folder.

**Note:** With CES 7.0.5935– (September 2013), the OCR module is available only in a 32-bit version, on a 64-bit server. The module components are installed by default in the C:\Program Files (x86)\Coveo Enterprise Search 7\OCR Module folder.

**Important:** The default OCR script configuration is a compromise between conversion completeness and performances and can prevent indexing some content in documents and possibly entire documents. Consider adapting the configuration to your needs (see "Tuning the OCR Module" on page 683).

4. Create a source to index the OCR documents (see "Adding a Source" on page 281).

5. Create an OCR open converter in CES:

a. On the Coveo server, access the Administration Tool.

b. Select Configuration > Converters > Open Converters.

c. In the Open Converters page, click Add.

d. In the Add an Open Converter page:
i. In the **Name** box, enter **OCR** as the name for the converter.

ii. In the **Script File** box, enter the path of the converter script file.

   **Example**: `C:\CES7\Scripts\OCRConversion7.js`

iii. In the **Script Language** drop-down list, select **JScript**.

iv. Click **Apply Changes**.

**What's Next?**

You must link the OCR open converter to document types in a document type set (see "Associating the OCR Open Converter to Document Types" on page 681).

### 8.9.2 Associating the OCR Open Converter to Document Types

After adding an open converter to CES, you must associate this converter to appropriate document types in a document type set. A typical configuration includes Adobe Acrobat documents (PDF) and image formats.

To associate the OCR open converter to document types

1. On the Coveo server, access the Administration Tool.

2. Select **Index > Sources and Collections**.

3. In the **Sources and Collections** page, select the source on which the OCR open converter script will be used. The **Status** page is displayed.

4. In the navigation panel on the left, click **Document Types**.

5. In the **Document Types** page, click **Add**.

6. In the **Add Document Type Set** page that appears:

   a. In the **Name** box, enter a name of your choice for the document type set to be used for indexing using the OCR module.
**Example: OCR Document Types**

b. In the **Description** box, optionally enter a description of the usage of the document type set.

c. Click **Save**.

7. Back in the **Document Types** page:

a. In the **Document Type Set** drop-down list, ensure that the document type set you just created is selected.

b. Click **Edit**.

8. In the page that appears, for each document type to be indexed using the OCR module:

a. Click the document type.

**Example: Click Adobe Acrobat Documents.**

**Note:** The document formats supported by the OCR module are: `.tiff`, `.tiff-fx`, `.pcx`, `.dcx`, `.bmp`, `.jpeg`, `.png`, `.max`, `.gif`, `.pbm`, and `.pdf`.

b. In the page that appears for this document type:
i. In the **Action** drop-down list, select **Index entire document**.

ii. In the **Converter** section, select **Use an open converter**, and then select the name of the converter that you created for this purpose (see "Adding an OCR Open Converter" on page 680).

iii. Click **Apply Changes**.

9. Open the CES Console (see "Using the CES Console" on page 246).

10. Back in the Administration Tool, rebuild the sources that use the new document type set.

11. In the CES Console, follow the rebuild activities. Documents are crawled, converted, and transactions are applied to index.

   The end-users can search for the OCR indexed document content once transactions are applied to the index.

8.9.3 Tuning the OCR Module

The OCR module comes with a default script (`OCRConverter7.js`) that you can modify to tune the default OCR conversion behavior. The default behavior is a compromise between converting as much content as possible
while limiting the time taken to process documents.

8.9.3.0.0.1 Default behavior you should know about

- PDF documents first go through the PDF converter. When the PDF converter finds a minimum amount of textual content in a PDF, the document is not sent to the OCR converter. Respecting this threshold prevents wasting time converting PDF documents containing text rather than images, but if some of your PDF documents contain both text and images, the module can miss content to be extracted by OCR. You can adjust the minimum amount of text using the mintextskippdfocr parameter that has a default value of 256 characters.

- By default, the OCR module only converts up to the first 200 pages of each document to prevent excessive conversion times. When you want all pages of all documents to be converted, you can increase the maxpage parameter value to ensure your longest PDF will be fully converted.

- By default, the OCR module only converts documents that are at least 10 KB in size, assuming these small documents (such as icons, logos, small images) do not contain images worth converting by OCR, and therefore save conversion resources. You can change this limit using the minsize parameter.

- When a document goes through the OCR converter, its converted output is put into the CES cache, so if you attempt to convert the same document again, to save conversion resources, the content of the cache is taken rather than converting the document again, even if you changed script parameters. When you try different conversion parameter values, you may think that the parameter changes had no effect, while they might if the document was actually converted.

When you convert again a set of documents, you can temporarily deactivate using the CES cache content for already indexed documents. In the OCRConverter7.js script file, as shown below, comment (add // in front of) lines 12 to 17 inclusively as well as line 43.

```javascript
// if (docCache.BytesCount > 0) {
//     // The OCR has already been done, copy the data in the OutputDocument.
//     docCache.SaveToFile(outputDocument);
//     CustomConversion.OutputDocument.LoadFromFile(outputDocument);
//     DocumentInfo.IsValid = true;
// } else {
//     ...
// }
```

To tune the OCR module conversion

1. Ensure you keep a intact copy of the original [CES_Path]\OCR Module\OCRConversion7.js script.

2. Using a text editor:
   a. Open your working copy of the OCRConverter7.js script.
   b. For parameters for which you want to use a value other than the default one, in function `image2Text.Init()` on line 21, add parameter-value pairs to the first semicolon separated string argument.

   ```javascript
   image2Text.Init("pdfloadflag=3; spellcheck=1; timeout=1200; language=en,fr,de,es;
   cleanuptmp=1; MaximumPixelsX=32000; MaximumPixelsY=32000", tempDirectory, parentProcess);
   ```

Refer to the following table, for available parameters.
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
<th>Default value</th>
<th>Maximum value</th>
</tr>
</thead>
<tbody>
<tr>
<td>cleanuptmp</td>
<td>Whether to delete OCR module generated temporary files. Consider setting to 0 for troubleshooting purposes to be able to inspect temporary file content.</td>
<td>1 (true - use 0 for false)</td>
<td></td>
</tr>
<tr>
<td>enginetimeout</td>
<td>OCR engine conversion timeout (milliseconds) for each call to the OCR API, such as when converting each page of a document, in which case the document is only indexed by reference (see &quot;What Is the Difference between Indexing by Reference and Indexing by Content?&quot; on page 481).</td>
<td>180000</td>
<td>-1 (no timeout)</td>
</tr>
</tbody>
</table>

Example: A log message when a `enginetimeout` occurs can look like:

```
Indexed by reference (Converter specific failure (The C:\CES7\Script\OCRConversionDev7D.js custom conversion script generated the following error: class CGLCOM::ActiveScript::Exception: CESCustomConverter.OCR.Debug.7.0 - Exception: class APICallFailedException: Error in OCR function kRecPreprocessImg With the following error code: API_TIMEOUT_ERR (line: 27, column: 8).))
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
<th>Default value</th>
<th>Maximum value</th>
</tr>
</thead>
<tbody>
<tr>
<td>language</td>
<td>Code of languages that the OCR module should recognize in the documents. Supported languages: ca, cs, da, nl, en, fi, fr, de, el, hu, it, no, pl, pt, sl, es, svd, ru, tr</td>
<td>en,fr,de,es</td>
<td></td>
</tr>
<tr>
<td>license</td>
<td>The OCR license file location.</td>
<td>[OCR_Install_Path]\license.txt</td>
<td></td>
</tr>
<tr>
<td>Parameter</td>
<td>Description</td>
<td>Default value</td>
<td>Maximum value</td>
</tr>
<tr>
<td>--------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>---------------</td>
<td>---------------</td>
</tr>
<tr>
<td>MaximumPixelsX</td>
<td>Required parameter specifying the maximum image width (in pixel) above which a document is not converted.</td>
<td>8400</td>
<td>32000</td>
</tr>
<tr>
<td></td>
<td><strong>Example: Related error message:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Indexed by reference (Converter specific failure (The C:\CES\Script\OCRConversionDev7D.js custom conversion script generated the following error: class CGLCOM::ActiveScript::Exception: CESCustomConverter.OCR.Debug.7.0 - Exception: class APICallFailedException: Error in OCR function kRecLoadImg With the following error code: IMG_SIZE_ERR. If converting big images, consider using the MaximumPixelsX and MaximumPixelsY parameters with values above the default value of 8400 in the Open Converter Script. (line: 27, column: 8).)) *</td>
<td></td>
<td></td>
</tr>
<tr>
<td>MaximumPixelsY</td>
<td>Required parameter specifying the maximum image height (in pixel) above which a document is not converted.</td>
<td>8400</td>
<td>32000</td>
</tr>
<tr>
<td>maxpage</td>
<td>Maximum number of pages converted for each document.</td>
<td>200</td>
<td>2147483647</td>
</tr>
<tr>
<td>maxretry</td>
<td>Maximum number of OCR engine initialization retries.</td>
<td>2</td>
<td>2147483647</td>
</tr>
<tr>
<td>minsize</td>
<td>Minimum document size (in bytes) below which documents are not converted by OCR.</td>
<td>10240</td>
<td>2147483647</td>
</tr>
<tr>
<td>mintextskippdfocr</td>
<td>For PDF documents only, the minimum number of characters found in the HTML generated by the PDF converter above which a PDF document is not processed by the OCR converter.</td>
<td>256</td>
<td>2147483647</td>
</tr>
<tr>
<td>Parameter</td>
<td>Description</td>
<td>Default value</td>
<td>Maximum value</td>
</tr>
<tr>
<td>-----------</td>
<td>-------------</td>
<td>---------------</td>
<td>---------------</td>
</tr>
<tr>
<td>ocrbinpath</td>
<td>Path of the OCR library binary files.</td>
<td>[OCR_Install_Path]</td>
<td></td>
</tr>
<tr>
<td>ocrbin64path</td>
<td>Path of the OCR library 64-bit version binary files.</td>
<td>[OCR_Install_Path]</td>
<td></td>
</tr>
<tr>
<td>pdfloadflag</td>
<td>Available PDF flag values: 1 - disable using PDF character codes. 2 - disable using PDF tags. 3 - process the PDF just as an image (without any PDF info). Flags can be OR-ed to combine the value of this setting. The recognition accuracy is usually worse if the value is 1 or 3.</td>
<td>2</td>
<td>3</td>
</tr>
<tr>
<td>spellcheck</td>
<td>Whether to use dictionaries available in several languages to improve the language detection.</td>
<td>0 (false - use 1 for true)</td>
<td></td>
</tr>
<tr>
<td>timeout</td>
<td>Whole document conversion timeout (seconds). When one occurs the document is only indexed by reference (see &quot;What Is the Difference between Indexing by Reference and Indexing by Content?&quot; on page 481).</td>
<td>600</td>
<td>2147483647</td>
</tr>
</tbody>
</table>

**Example:** A log message when a timeout occurs can look like:

```
Indexed by reference (Converter specific failure (The C:\CES7\Script\OCRConversionDev7D .js custom conversion script generated the following error: class CGLCOM::ActiveScript::Exception: CESCustomConverter.OCR.Debug.7.0 - OCRS timeout. (line: 27, column: 8).))
```

c. Save the file.

3. Consider enabling the OCR logs to get more feedback on the conversion process:

   In the C:\tmp folder, add a dummy empty file with the name OCR_TRACE_FLAG.flag. Additional OCR information will be logged in the C:\tmp\ocr_tracefile.log file.
What's Next?

Ensure your modified `OCRConverter7.js` script is the one used by your OCR open converter (see "Adding an OCR Open Converter" on page 680).

8.10 Text Analytics Module

Text analytics is a process that helps to better exploit unstructured information by adding structure to the content in the form of new metadata values. The optional Coveo Text Analytics module allows you to analyze and tag indexed documents containing specific information. Once this information is in the index, you can use it to create facets, provide relevant query suggestions, analyze, consolidate and correlate documents and trends to offer a better insight to the end-user.

8.10.1 Text Analytics Application Examples

The following are examples where text analytics can be applied and provide great benefits.

**Improved navigation with topic-based facets**

End-users can efficiently drill down to documents they are looking for using facets. You can use text analytics to extract *themes* and *named entities* and create facets based on this information to improve search results navigation.

**Expertise finding**

Finding experts on a subject or domain is a need found in many organizations. Text analytics can help identify experts based on dynamic analysis of how people in an organization are linked to content (authors, owners, mentioned in, linked to).

**Improved efficiency of customer service agents**

Customer service agents generally need to find answers and solutions to client's issues from a large number of structured and unstructured content sources. You can use text analytics to extract many relevant information types from case descriptions, knowledge base articles, wikis, issue tracking systems, emails, etc. When an agent opens a case, Smart Relations lists automatically present related content from various sources.

**Customer review analysis**

Knowing what clients think of products is key information to all successful businesses. You can use text analytics to extract company names, product names, themes and perform sentiment analysis on customer review sites or forums, and then create facets based on this metadata. Product management people can then easily analyze what customers like and dislike about their company's products and those of their competitors.
Example: In the following Knowledge Base console, the user searched for `firmware` and gets matching knowledge base articles in the middle of the screen. The user can then use the facets on the left to refine search results and review related information from other sources on the right. Text analytics is behind several insightful user interface elements of this console.

1. **Product** facet based on the extracted `Product` named entity.
2. **Theme** facet based on the extracted `Themes`.
3. **List of Experts** built by linking extracted `People` named entity with keywords and `Themes`.
4. **List of Resolved Tickets** from issue tracking system sharing similar extracted `Themes` as the current search results.
5. **List of posts from Communities** sharing similar extracted `Themes` as the current search results.

### 8.10.2 Module Components

The installer of the Text Analytics module deploys the following components:

- **TAnGO administration tool**
  
  A tool used to register, setup, and manage text analytics configurations (see "TAnGO Administration Tool" on page 693).
- Coveo Job Scheduling (CJS) service
  The service responsible for launching and monitoring runs and jobs (see "Coveo Job Scheduling Service" on page 691).

- Predefined run and job pipeline plugins
  A set of useful plugins that you can assemble as building blocks to easily create a complete text analytics pipeline (see "Text Analytics Run Plugins" on page 713 and "Predefined Text Analytics Job Plugins" on page 727).

- Entity discovery plugin
  A text analytics pipeline can use an entity discovery plugin (Salience) to extract themes and named entities as well as perform sentiment analysis from documents (see "Entity Discovery Plugin" on page 690).

- Text analytics developer framework
  The CustomImplementations C# framework includes the code of all predefined plugins (see "Text Analytics C# Developer Framework" on page 695).

Text Analytics Module - Feature History

<table>
<thead>
<tr>
<th>Version</th>
<th>Date</th>
<th>Features</th>
</tr>
</thead>
<tbody>
<tr>
<td>2.0.13+</td>
<td>November 2012</td>
<td>Addition of the LoggingVerbosity pipeline global configuration parameter (see &quot;Text Analytics 2.0.13+ (November 2012)&quot; on page 712).</td>
</tr>
</tbody>
</table>
| 2.0.11+ | October 2012  | - Addition of the FetchBatchSize pipeline global configuration parameter (see "<FetchBatchSize>" on page 712).  
- Addition of new predefined job plugins (see "MasterFieldMoverJob" on page 728, "ClearFieldJob" on page 728). |

8.10.3 Entity Discovery Plugin
The entity discovery plugin can extract themes and named entities and perform sentiment analysis on textual content.

8.10.3.1 Themes

*Themes* are noun phrases extracted from full text based on linguistic analysis. A noun phrase is a sequence of one or more terms that can be replaced by a noun or pronoun. The entity discovery plugin typically extracts 2-word themes.

**Example:** The expression *community account management* is a sequence of terms that can be replaced by it, and could therefore be extracted as a theme.

Theme extraction works best on documents containing regular text made of complete sentences and not very well on documents containing text chunks such as log files.

The relevance of a theme extracted for a single document is magnified when appearing in a correlation ranked facet, allowing end-users to easily pull subject related documents from dispersed sources.
8.10.3.2 Named Entities

Named entities are unique text elements that can be classified in predefined categories. The entity discovery plugin can extract named entities for a fair number of categories (company names, product names, people, job titles, places, dates...). When found in a document, named entity values are saved as metadata named after the corresponding category and attached to the document.

Example: With named entity extraction enabled, when processing the following sentence:

This article comments Paul Baker's favorite restaurants in Boston.

The following metadata and values are created for this document:

- People = Paul Baker
- Place = Boston

With named entity extraction enabled, the entity discovery plugin always generates metadata for all categories that it supports and finds. In the text analytics pipeline, you can use a filter plugin to only pass metadata from named entity categories of interest to the outputter stage (see “SalienceMetadataExtractor” on page 719 and “MetadataFilter” on page 722).

Facets using named entities allow end-users to easily find documents referring to specific name entities.

8.10.3.3 Sentiment Analysis

The entity discovery plugin can use the optional Sentiment Analysis feature to calculate an overall sentiment score for a document by finding predefined expressions associated with positive or negative sentiment and summing their respective sentiment scores. Sentiment analysis produces best results with full sentence content that is likely to include judgments, opinions, or moods such as posts from customer review communities.

Example: With sentiment analysis enabled, when processing the following sentence:

This is the worst and most painful software installation I ever went through. However, once installed, its features are nice.

An overall negative sentiment is returned since the terms worst and most painful carry a significantly negative score compared to the word nice that carries a positive score. Other terms are neutral as they do not carry sentiment.

By default, sentiment analysis returns either positive, neutral, or negative sentiment. You can however configure multiple-levels and customize the sentiment level names (see “SalienceMetadataExtractor” on page 719).

8.10.4 Coveo Job Scheduling Service

The installer of the Text Analytics module deploys and registers the Coveo Job Scheduling (CJS) service as a Windows service so that you do not have to worry about starting it. The CJS service registers and manages execution of text analytics tasks in the form of runs and jobs (see "Runs Versus Jobs" on page 710).

When starting the CJS service for the first time, the [Text_Analytics_Path]CJS folder and the schedule configuration file (SchedulerConfig.jbf) are automatically created. No text analytics pipeline is registered by
default. You can use the TAnGO administration tool to easily create, register, and run text analytics tasks once or at regular time intervals (see "Managing Text Analytics Pipeline Configurations" on page 707).

The CJS service logs information in its own folder. When you register a new task using TAnGO or the command line, the scheduler saves the path of the pipeline configuration file together with other information required to launch the tasks.

8.10.4.1 Standalone Mode

You can also start the service in standalone mode. This mode is useful when you build and test your text analytics pipeline in a development environment.

You can start the CJS service in standalone mode from a command prompt, using the following command:

```
[Text_Analytics_Path]\Bin\CJSService2.exe -standalone
```

The CJS service console window appears.

Note: The Windows Firewall may block some features of the CJS service. In this case, select your network and then click Allow Access.

8.10.4.2 Command Line Options

From a command prompt, you can get the list of CJS service command line options by launching the CJS service executable with no arguments:

```
[Text_Analytics_Path]\Bin\CJSService2.exe
```

The following window appears.
8.10.5 TAnGO Administration Tool

The Text Analytics module comes with the TAnGO (Text Analytics ‘n GO) administration tool that allows you to easily manage text analytics tasks.
1 Toolbar from which you can **Register**, **Duplicate**, **Unregister**, **Run**, or **Stop** text analytics runs and jobs.

2 Panel presenting the list of currently registered text analytics runs and jobs.

3 **Job Logs** panel presenting the logs of the currently selected run or job allowing you to monitor its progress.

4 Connection status with the Coveo Job Scheduling service and link to its **Settings**.

5 **Create Configuration File** button allowing you to easily create a new text analytics pipeline (see "Creating a Custom Run or Job from a Template" on page 707)

6 **Job details** panel presenting status information of the currently selected run or job, and allowing you to edit the state (see "Reprocessing All Documents with a Text Analytics Run" on page 732).

### 8.10.5.1 Starting TAnGO

You can start TAnGO using one of the following methods:

- From the Windows **Start** menu, select **All Programs > Coveo Text Analytics 2 > TAnGO**.
OR

- From a command line:
  1. From the Windows **Start** menu, select **All Programs > Accessories > Command Prompt**.
  2. In the Command Prompt window, change to the `[Text_Analytics_Path]\Bin\` folder, type `TAnGO`, and then press Enter.

### 8.10.6 Text Analytics C# Developer Framework

The Text Analytics module comes with a set of files that allows programmers from your organization or from a third party to easily start developing custom text analytics features. The files are available in the `[Text_Analytics_Path]\SDK\Custom.TextAnalytics.Implementations\` folder.

The package includes:

- A **Visual Studio project file** *(Coveo.TextAnalytics.Implementations.Custom.csproj)*
- Code for all predefined run and job plugins

### 8.10.7 Text Analytics Module - Deployment Overview

**CES 7.0.4863+ (September 2012)**

This topic presents the main tasks to deploy the Text Analytics module.

To deploy the Text Analytics module

1. Ensure that you use a Coveo Enterprise Search version 7.0.4863+ that is fully compatible with the Text Analytics module version 2.0.5+.

2. After acquiring the optional Text Analytics module, ensure that you received the following information from Coveo (if not contact **Coveo Support**):
   - Coveo license file supporting text analytics and super user access
   - License file for the entity discovery plugin (Salience)
   - Link to download the installer of the Text Analytics module

3. Ensure that your Coveo Master server uses the Coveo license with text analytics support.

**CES 7.0.4887+ (November 2012)** In the Administration Tool, go to the **Configuration > License** page, and verify that a check mark appears next to **Text Analytics Allowed**.
Note: When the Coveo license does not support text analytics and you attempt to run a text analytics run or job, the Text Analytics is not allowed by CES license message appears in the TAnGO Job Logs panel.

4. Select or create a user to run the text analytics processes:
   a. Select or create an Active Directory domain user that you will set later to run the Coveo Job Scheduling (CJS) service that manages text analytics runs and jobs.

   Account requirements:
   - Dedicated to Coveo processes
   - Password that never changes to prevent access errors.

   Note: If you must use an account with a password that must change regularly, you will need to also change the password for Coveo Job Scheduling Service 2 (Text Analytics) in Windows Services whenever it changes in Active Directory.

   Tip: Use the same account as the one running the CES service.

   b. Grant super user access (with the Access Everything option selected) to the account to ensure that the text analytics processes have read access to all indexed documents. Note the super user ID. You will need it later.

5. Install the Text Analytics module (see "Installing the Text Analytics Module" on page 697).

6. Set the basic parameters needed by all the text analytics runs and jobs (see "Performing the First Time Setup of the Text Analytics Module" on page 700).

7. Ensure that the installation and configuration allows the text analytics module to produce usable outputs:
   a. Use an out-of-the-box run template to produce your first text analytics tag fields in the unified index (see "Testing the Text Analytics Installation" on page 703).

   b. Take advantage of text analytics output in your .NET search interface by adding facets based on the newly created tag fields.
Example: Create a facet that lists the places found in your documents using the \texttt{@txtanplace} tag field. The facet allows end-users to easily find documents referring to selected locations.

8.10.7.1 Installing the Text Analytics Module

The installer of the Text Analytics module allows you to easily install all the components of the module. You typically install the Text Analytics module on the Coveo Master server.

\textbf{Note:} Consider installing the module on a separate server only when CES and Text Analytics processes compete for server resources and start to affect server performances. Text analytics operations can be CPU intensive and can impact performances of a Coveo Master server that is already busy indexing content or serving queries.

To install the Text Analytics module

1. Using an administrator account, connect to the server on which you want to install the Text Analytics module.

2. Download the latest version of the Text Analytics installer, depending on your license:
   - \texttt{TextAnalytics x64}
   - \texttt{TextAnalytics with Salience x64} when your license include the Salience Engine

\textbf{Note}: If you are still running on a 32-bit server, Win32 versions of the Text Analytics module are also available. Contact Coveo Support to get these installers.

3. Execute the Text Analytics installer:
   a. In the welcome screen, click \textbf{Next}.
   b. In the \textbf{Select Destination location} screen, when you want to install the files in a folder other than the default folder (\texttt{c:\TextAnalytics}), click \textbf{Browse} to select the installation folder, and then click \textbf{Next}. 
c. In the **Configure Job Scheduling service account** screen, enter the credentials (Domain, Username, and Password) for the Active Directory account that you chose to use, and then click **Next**.

**Note:** The Text Analytics module does not support using a local account.

d. In the **Ready to Install** screen, click **Install**.

e. In the **Completing the Coveo Text Analytics Setup Wizard** screen, select the Run configuration utility check box, and then click **Finish**.
4. The TAnGO Coveo Text Analytics Configuration window appears. In the upper-right corner, ensure that the status of the connection between TAnGO and the Coveo Job Scheduling service is **Service: Connected**.

If it is not the case:

- Ensure that the Coveo Job Scheduling service runs as a Windows service or in standalone mode (see "Coveo Job Scheduling Service" on page 691).
- Click the **Settings** link and verify that TAnGO is looking for the Coveo Job Scheduling service on the
correct machine and port.

![Service Settings](image)

**What's Next?**

Perform the initial configuration of the Text Analytics module (see "Performing the First Time Setup of the Text Analytics Module" on page 700).

### 8.10.7.2 Performing the First Time Setup of the Text Analytics Module

Once the Text Analytics module is installed, you must configure the location of required files and the connection to Coveo Enterprise Search (CES). This configuration generally only needs to be done once.

To perform the first time setup of the Text Analytics module

1. On the server where your installed the Text Analytics module:
   a. Copy the entity discovery plugin license file (license.v5) that you received from Coveo to the [Text_Analytics_Path]\Lexalytics\ folder.
   b. If you installed the module on a server other than the Coveo Master server:
      i. From the Coveo Master server, copy the a search security certificate file used by your Coveo Front-End server(s) (such as [Index_Path]\Config\Certificates\cert-iis.p12).
      ii. On the server where the Text Analytics module is installed, paste the certificate file in a text analytics subfolder of your choice.

   **Example:** Create the D:\TextAnalytics\CES_Certificates\ folder, and then paste the certificate file in it.

2. Start TAnGO (see "Starting TAnGO" on page 694).
3. In TAnGO, click **Create Configuration File**.

4. In the **Create New Configuration File** dialog box:
a. In the **Text Analytics** section, under **Salience**, in the **License** box, ensure that the path/filename points to the entity discovery plugin license file that you saved earlier.

b. In the **CES** section, under **Server Information**:

i. In the **Host** box, when you installed the Text Analytics module on a server other than the Coveo Master server, enter the name of the Coveo Master server, otherwise, leave **localhost**.

ii. When CES uses a port other than the default one (52800), in the **Port** box, enter the port used.

iii. In the **Certificate** box, ensure that the path points to the location of a valid search security certificate file.

iv. In the **Super User Token** box, paste the **ID** of the super user account that you created and copied earlier for the Text Analytics module.

c. Still in the **CES** section, under **Admin Service Credentials**, enter the credentials of the administrator account to use (**Domain\Username** and **Password**).
Note: This account must have CES administrator permissions as it communicates with the CES administration web service to perform tasks such as license status verification and tag field creation. If the password changes, you must recreate the configuration.

d. Click **Save**.

e. In the **Save Configuration File as** dialog box, browse to the `[Text_Analytics_Path]\Config\` folder, in the **File name** box enter a name of your choice (ex: `FirstTimeSetup`), and then click **Save**.

The parameters that you configured in this procedure will be automatically included in new pipeline configuration files that you create using templates.

What's Next?

Ensure that your text analytics installation and configuration is operational (see “Testing the Text Analytics Installation” on page 703).

8.10.7.3 Testing the Text Analytics Installation

Once both the text analytics installation and first time setup are completed, you can use one of the out-of-the-box templates to validate that your text analytics implementation is operational.

To test the text analytics installation

1. Using an administrator account, connect to the server on which the Text Analytics module is installed.

2. Start TAnGO (see “Starting TAnGO” on page 694).

3. In TAnGO, click **Create Configuration File**.

4. In the **Create New Configuration File** dialog box:
a. In the **Text Analytics** section, under **Paths**, in the **Configuration Template** box, browse to select one of the out-of-the-box run or job templates available in the [Text_Analytics_Path]\Config\ folder.

**Example:** By default, the run-Template.xml file extracts themes, places, person names, and company names, and then tags documents containing those using new tag fields (@txtantheme, @txtantheme, @txtanplace, @txtanperson, and @txtancompany).

b. Click **Save and Register**.

c. In the **Save Configuration File as** dialog box, browse to the [Text_Analytics_Path]\Config\ folder, in the **File name** box enter a name of your choice (ex: run-TemplateTest), and then click **Save**.

5. In TAnGO:
a. In the top-left panel, click your run or job to see its state in the **Job Details** panel.

b. When the run or job starts following the time interval schedule, in the **Job Logs** panel, verify that logged activities appear to run smoothly.

c. If error messages appear, review the installation and first time setup steps to fix them (see "Installing the Text Analytics Module" on page 697 and "Performing the First Time Setup of the Text Analytics Module" on page 700).

**What's Next?**

Take advantage of text analytics output in your .NET search interface by adding facets based on the newly created tag fields.

**8.10.8 Text Analytics Pipeline Configuration**

Text analytics operations are defined in a pipeline consisting of one or more stages. The pipeline stages are defined in an XML configuration file that starts with a global configuration section (see "Text Analytics Global Configuration Parameters" on page 711). Each XML configuration file can define one or more text analytics runs or jobs (see "Runs Versus Jobs" on page 710).

Text analytics pipelines are registered in the Coveo Job scheduler (CJS) service using TAnGO (see "Managing Text Analytics Pipeline Configurations" on page 707). The CJS service manages the launch of a pipeline once or at specified regular intervals.

**8.10.8.1 About Runs**

A **run** is a text analytics pipeline that sequentially applies a set of stages on a set of documents.
**Example:** Typically, a set of documents is fetched from the Coveo unified index, text analytics metadata is extracted, and the metadata is injected back in the index in the form of tag fields.

The pipeline is composed of stages of the following types in the following order:

**Fetcher**

A run always starts with a fetcher plugin that retrieves documents to be processed by the pipeline (see "Predefined Text Analytics Fetcher" on page 713). There can be only one fetcher plugin in a pipeline.

**Filters**

The pipeline can contain one or more filter plugins used to exclude specific type of content from the fetched documents, before they are processed further (see "Predefined Text Analytics Filters" on page 715).

**Extractors**

At the center of the text analytics process, one or more extractor plugins create and attach metadata to processed documents (see "Predefined Text Analytics Extractors" on page 716).

**Normalizers**

One or more normalizer plugins clean-up the metadata created by the extractors (see "Predefined Text Analytics Normalizers" on page 722).

**Outputter**

At the end of the pipeline, an outputter plugin saves the text analytics results somewhere. There can be only one outputter plugin in a pipeline (see "Predefined Text Analytics Outputters" on page 724).

The pipeline structure for a run is shown in the following XML configuration file sample.

```xml
<?xml version="1.0" encoding="utf-8"?>
<TextAnalyticsService>
  <!-- Global configuration parameters -->
  <Configuration>
    ...
  </Configuration>
  <!-- Definition of the run -->
  <Run Name="MainRun">
    <!-- Plugin used to fetch the documents to process -->
  </Run>
</TextAnalyticsService>
```
8.10.8.2 About Jobs

A job is a one stage pipeline that you can use when you need to execute general tasks that should not be executed on each individual document.

Example: You can use a job when you want to use CES tagging queries, copy files, programmatically change a configuration in CES, perform a maintenance task, etc.

What’s Next?

Review the procedure to create, run, and fine-tune text analytics pipelines (see "Managing Text Analytics Pipeline Configurations" on page 707).

8.10.8.3 Managing Text Analytics Pipeline Configurations

Once you successfully deployed your Text Analytics module and understand what a pipeline is, you can start creating, running, and fine-tuning your own text analytics pipelines.

8.10.8.3.1 Creating a Custom Run or Job from a Template

You can easily create a typical pipeline configuration with pre-populated values for many parameters starting from a template. Run or job template files contain placeholder variables for many parameter values that are automatically filled with appropriate values when you create a configuration using them.

To create a custom run or job from a template

1. Start TAnGO (see "Starting TAnGO" on page 694).
2. In TAnGO, click Create Configuration File.
3. In the Create New Configuration File dialog box:
a. In the **Text Analytics** section, under **Paths**, in the **Configuration Template** box, select the run or job template file on which you want to base your custom configuration.

b. Click **Save**.

c. In the **Save Configuration File as** dialog box, browse to the `[Text_Analytics_Path]\Config\` folder, in the **File name** box enter a name of your choice for your custom pipeline (ex: *MyFirstPipeline*), and then click **Save**.

4. Using a text editor:

a. Open the pipeline configuration file that you just created.

b. Respecting the XML format of the file and of available plugins, modify or remove existing plugins or add new ones to achieve desired results (see "Text Analytics Run Plugins" on page 713 and "Predefined Text Analytics Job Plugins" on page 727).

c. Save the file.
8.10.8.3.2 Running a Custom Run or Job

1. Start TAnGO (see "Starting TAnGO" on page 694).

2. In TAnGO:
   a. Click **Register**.
   b. In the **Open Configuration File** dialog box, select the configuration file for the custom run or job that you want to execute, and then click **Open**.

The selected pipeline starts to run once or at scheduled time intervals.

8.10.8.3.3 Fine-Tuning the Text Analytics Output

Once you ran your custom pipeline, fine-tuning the output is often an iterative process involving adding and tuning plugins until the desired output is achieved.

To fine-tune the text analytics output

1. Inspect the output of your text analytic pipeline.

   **Example:** In your search interface, create facets based on fields created by your text analytics pipeline. Inspect the item of these facets.

2. In a run, when unnecessary or too much content is processed:
a. Consider tuning the fetcher plugin to better scope the document set to process (see "Predefined Text Analytics Fetcher" on page 713).

b. Consider using filters to exclude part of the fetched content before proceeding with the extraction (see "Predefined Text Analytics Filters" on page 715).

3. When you want to find and tag documents containing specific text strings, consider creating a white list that includes these values and add a whitelister plugin to the pipeline (see "Whitelister" on page 716).

4. When unwanted values appear in extracted metadata, consider creating one or more blacklist files and adding one or more blacklister plugins to eliminate the unwanted occurrences (see "MetadataBlackLister" on page 722).

5. When two or more values of extracted metadata correspond to a unique element, consider adding one or more normalizer plugins to homogenize metadata values (see "MetadataNormalizer" on page 723).

8.10.8.4 Runs Versus Jobs

The Text Analytics module can perform operations either as a run or as a job. The following table summarizes the similarities and the differences between the two types of operations.

<table>
<thead>
<tr>
<th>Aspect</th>
<th>Run</th>
<th>Job</th>
</tr>
</thead>
<tbody>
<tr>
<td>Brief definition</td>
<td>Sequence of pipeline stages iteratively executed on a set of documents.</td>
<td>Executes a piece of code to perform any task and does not operate on a set of documents.</td>
</tr>
<tr>
<td>Executed</td>
<td>By the Coveo Job Scheduling (CJS) service</td>
<td></td>
</tr>
<tr>
<td>When to use</td>
<td>• Operations must be performed on each document of a set, one at a time.</td>
<td>• One shot operation such as maintenance tasks like creating a backup, checking something, granting permissions, creating tag fields in the Coveo unified index, etc.</td>
</tr>
<tr>
<td></td>
<td>• To initially process all indexed documents and process new, deleted, or changed indexed documents at regular intervals.</td>
<td>• To whitelist, blacklist, or normalize known values in all documents using tagging queries.</td>
</tr>
<tr>
<td>Performance</td>
<td>• Dependent on document set size and the number and resources required by each pipeline</td>
<td>• Dependent on the code of the plugin</td>
</tr>
<tr>
<td></td>
<td>• Changes in the pipeline normally require to reprocess all documents in the pipeline, one by one.</td>
<td>• Changes to whitelists, blacklists, and normalizers can be quickly applied to the index since each modification is applied on all specified documents simultaneously using CES tagging queries.</td>
</tr>
</tbody>
</table>
Example: After completing a text analytics run that processed all documents in your Coveo unified index, you need to normalize or blacklist extracted items. To do so:

1. Add the necessary terms to blacklisting and normalization files.
2. Add the blacklisting and normalization plugins using these files to your run so upcoming scheduled executions will blacklist and normalize terms for new index documents.
3. Use a job to efficiently perform normalization and blacklisting for the index documents that have already been processed.

8.10.8.5 Text Analytics Global Configuration Parameters

Text analytics global configuration parameters apply to the run(s) and job(s) defined in the current configuration file. The values of several global configuration parameters are automatically set when you use a template to create a new configuration file (see "Creating a Custom Run or Job from a Template" on page 707).

Global configuration parameters:

<Continuous>

Set this parameter to True to launch the run at a regular time interval specified in the <SleepBetweenRuns> parameter. Activate the continuous mode when you want to process new indexed documents at regular intervals. The launch is canceled when the run is already active.

<SleepBetweenRuns>

This parameter specifies the time interval in milliseconds (ms) between runs when the <continuous> parameter is set to True. Select a time interval that is long enough to ensure that a typical incremental run completes within the time interval, and short enough to ensure new indexed documents are readily processed to maintain the text analytics data freshness without wasting CPU resources.

<NbThreads>

This parameter specifies the number of threads that the pipeline can use. Using more than one thread is particularly useful with CPU intensive extractors such as the SalienceMetadataExtractor. Text analytics processing such as theme and named entity extraction can be CPU intensive. Select the number of threads to be equal to the number of CPU cores that you can afford to devote to text analytics.

<StateDir>

For runs only, this parameter specifies the folder where the pipeline state is saved in a cookie file. When using the CESIQuerierFetcher, the state contains the rowid of the last processed document. The default value is [Text_Analytics_Path]\Config\state\.

<ThemeMetaName>

For runs only, this parameter is required to specify the name to use for the Themes metadata when the pipeline includes the SalienceMetadataExtractor plugin (see "SalienceMetadataExtractor" on page 719).

<SentimentMetaName>

For runs only, this parameter is required to specify the name to use for the Sentiment metadata when the pipeline includes the SalienceMetadataExtractor plugin (see "SalienceMetadataExtractor" on page 719).
<CESCertificatePath>

This parameter specifies the folder and the filename of the valid Coveo Enterprise Search (CES) search security certificate that the module must use to be able to fetch documents from the unified index. The default value is [Index_Path]\Config\Certificates\cert-iis.p12.

When the Text Analytics module is installed on a server other than the Coveo Master server, ensure that the path and file name correspond to where you copied the file (see "Performing the First Time Setup of the Text Analytics Module" on page 700).

Example: When the Text Analytics module is installed on the Coveo Master server, the default is:
<CESCertificatePath>C:\ces7\Config\Certificates\cert-iis.p12</CESCertificatePath>

<CESSearchHost>

This parameter specifies the address of the Coveo Master server to use to fetch and tag indexed documents. You can enter localhost when the Text Analytics module is installed on the Coveo Master server.

<CESSearchPort>

This parameter specifies the port to use on the Coveo Master server to fetch and tag indexed documents. The default value is 52800.

<SuperUserToken>

This parameter specifies the super user ID that the user running the Coveo Job Scheduling service must pass to CES to be able to fetch all indexed documents. Paste the super user ID that you created (see "Text Analytics Module - Deployment Overview" on page 695).

Example: Your super user ID is an hexadecimal GUID similar to this one: <SuperUserToken>e401b92d-0f40-4b44-a85e-0eb56d9e06c2</SuperUserToken>

<FetchBatchSize>

This parameter specifies the number of documents fetched from the unified index by the CESIQuerierFetcher plugin for each batch. The default value is 100 and the maximum value is 1000. This parameter is available in Text Analytics version 2.0.11+.

Text Analytics 2.0.13+ (November 2012)

This parameter specifies the level of details that is logged. The default value is All. Other options are: WarningsAndErrors and ErrorsOnly.
Example: The following configuration file sample shows the global configuration section as it appears in a run template where placeholders in the %[Parameter value]%% format will be replaced by appropriate values when you create a pipeline configuration file using TAnGO (see "Creating a Custom Run or Job from a Template" on page 707).

```xml
<?xml version="1.0" encoding="utf-8"?>
<TextAnalyticsService>
  <!-- Global configuration parameters -->
  <Configuration>
    <!-- The run will execute continuously, looking for new documents to process after the first pass is completed. Waits SleepBetweenRuns (in ms) before checking for new results to process -->
    <Continuous>True</Continuous>
    <FetchBatchSize>100</FetchBatchSize>
    <SleepBetweenRuns>30000</SleepBetweenRuns>
    <NbThreads>2</NbThreads>
    <!-- The name of the metadata for themes -->
    <ThemeMetaName>Theme</ThemeMetaName>
    <!-- Location of the file used to save the value of the ID of the latest processed document -->
    <StateDir>%TextAnalyticsRootDirectory%\Config\state</StateDir>
    <CESSearchPort>%CESSearchPort%%</CESSearchPort>
    <CESCertificatePath>%CESCertificateFile%%</CESCertificatePath>
    <!-- Super user token used to provide read access to all indexed documents to the text analytics processes. -->
    <SuperUserToken>%CESSuperUserToken%%</SuperUserToken>
  </Configuration>
  <!-- Definition of the run -->
  <Run Name="MainRun">...
  </Run>
</TextAnalyticsService>
```

What's Next?

Look at the available predefined run and job plugins (see "Text Analytics Run Plugins" on page 713 and "Predefined Text Analytics Job Plugins" on page 727).

8.10.8.6 Text Analytics Run Plugins

The Text Analytics module comes with a set or predefined plugins that you can use in a run. The available plugins are grouped by stage type.

8.10.8.6.1 Predefined Text Analytics Fetcher

One and only one fetcher stage must appear at the beginning of a text analytics pipeline. The fetcher is responsible for getting the document set on which the pipeline will operate.

There is currently only one predefined fetcher plugin available.

8.10.8.6.1.1 CESIQuerierFetcher

The CESIQuerierFetcher fetcher retrieves documents from the Coveo unified index to assemble the document set that the text analytics pipeline will process. Use the following parameters to configure the fetcher.

```xml
<AddTitle>
<AddBody>
  By default, the title and the body of each document are added to the content to be processed. You can set these
```
optional parameters to False to prevent these inclusions.

**Note:** AddBody works only when a Quick View is available for the indexed documents. You must select the Generate a cached HTML version of indexed documents source option to create document Quick Views.

### <AddField>

Optionally, you can set one or more instances of this parameter to add the content of textual (string type only) custom and system fields to the process content.

### <Query>

This parameter scopes the retrieval of the documents by specifying a valid query.

**Examples:**

- `@syscollection=Intranet`
  Retrieves only documents from the Intranet collection.
- `@syssource="CRM"`
  Retrieves only documents from the CRM source.
- `@syslanguage=English`
  Retrieves only English documents.

### <SaveState>

This parameter must be set to True for continuous runs. The @sysrowid field value of the last processed document is saved in a cookie file specified in the <StateFolder> global configuration parameter (see "Text Analytics Global Configuration Parameters" on page 711).

### <SaveStateFrequency>

This parameter specifies the number of documents to process between each saving of the @sysrowid field value in the file specified in the <StateFolder> global configuration parameter. By default, the state is saved every 30 documents to prevent writing to the file too often.

**Example:**

```xml
<Fetcher>
  <Impl>Coveo.TextAnalytics.Implementations.CESIQuerierFetcher,
  Coveo.TextAnalytics.Implementations</Impl>
  <Configuration>
    <!-- Scope which documents to retrieve -->
    <Query>@uri</Query>
    <SaveState>True</SaveState>
    <SaveStateFrequency>30</SaveStateFrequency>
    <AddTitle>True</AddTitle>
    <AddBody>True</AddBody>
    <AddField>@myfield</AddField>
    <AddField>@anotherfield</AddField>
    <!-- A valid CES certificate is needed to search and retrieve documents -->
    <CertificatePath>C:\ces7\Config\Certificates\cert-iis.p12</CertificatePath>
  </Configuration>
</Fetcher>
```
8.10.8.6.2 Predefined Text Analytics Filters

Filter plugins are responsible for removing specific type of content from each fetched document to prevent to process them in the rest of the pipeline. They are used between the fetcher stage and extractor stage.

8.10.8.6.2.1 LongNonSentenceLinesFilter

The LongNonSentenceLinesFilter plugin determines whether a BLOB of text is structured like a sentence by checking the presence of punctuation, spaces, etc. When it is not the case, such as for a folder path or a line of programming language code, the BLOB of text is removed from the content sent to the rest of the pipeline. This filter is useful to prevent sending non-phrasal content to the entity discovery plugin that could consume significant CPU resources on the BLOB of text and extract no information. This filter does not have parameters.

```xml
<Filter>
  <Impl>Coveo.TextAnalytics.Implementations.LongNonSentenceLinesFilter,
  Coveo.TextAnalytics.Implementations</Impl>
  <Configuration>
  </Configuration>
</Filter>
```

8.10.8.6.2.2 NonSentenceFilter

The NonSentenceFilter plugin analyzes each line of text and determines if it is a valid English sentence based on word lookup such as stop words (a, the, of...) and statistical analysis (number of symbols, numbers, etc.). When the line is found to not be a sentence, the line is removed from the content sent to the rest of the pipeline. This filter is useful to prevent sending non-phrasal content to the entity discovery plugin that could consume significant CPU resources on the BLOB of text and extract no information. This filter does not have parameters.

```xml
<Filter>
  <Impl>Coveo.TextAnalytics.Implementations.NonSentenceFilter,
  Coveo.TextAnalytics.Implementations</Impl>
  <Configuration>
  </Configuration>
</Filter>
```

8.10.8.6.2.3 RegexLineFilter

The RegexLineFilter plugin evaluates each line of processed documents against one or more regular expressions (regex) defined by the <Regex> parameter. If any one of the regexes matches the line, the line is removed from the content sent to the rest of the pipeline. This filter is generic and powerful, but can require significant CPU resources when specifying complex regular expressions.

.example: The following filter removes lines starting with the # symbol.

```xml
<Filter>
  <Impl>Coveo.TextAnalytics.Implementations.RegexLineFilter,
  Coveo.TextAnalytics.Implementations</Impl>
  <Configuration>
    <Regex>^[^#].*$</Regex>
    </Configuration>
</Filter>
```
8.10.8.6.2.4 EmailHeaderFilter

The EmailHeaderFilter plugin removes email header lines starting with From:, Sent:, Subject:, To:, and Importance:. In general in the index, the email body retrieve by the fetcher does not include header lines. This filter is useful in rare cases where indexed email documents include the email header lines and you want to process these email messages without the header content. Note that the subject is generally set as the document title so it is still processed even if the Subject: line is removed. This filter does not have parameters.

```xml
<Filter>
  <Impl>Coveo.TextAnalytics.Implementations.EmailHeaderFilter,
  Coveo.TextAnalytics.Implementations</Impl>
  <Configuration/>
</Filter>
```

What's Next?

Evaluate available extractors (see "Predefined Text Analytics Extractors" on page 716).

8.10.8.6.3 Predefined Text Analytics Extractors

The extractor stage is at the center of the text analytics process. Extractor plugins identify and extract specific types of information from the content of the processed documents.

8.10.8.6.3.1 Whitelister

The Whitelister plugin reads a flat text file containing a list of expressions, one per line. Each expression is searched in each processed document. When there is a match, the term is added as a metadata to the document. The listed expressions must match word boundaries. Only exact matches are extracted. Case sensitivity can be set.
Example: The following Whitelister plugin populates the ToyotaVehicles metadata with occurrences of expressions found in the ToyotaVehicleList.txt file.

```xml
<Extractor>
  <Configuration>
    <MetadataName>ToyotaVehicles</MetadataName>
    <FilePath>D:\TextAnalytics\Config\whitelists\ToyotaVehicleList.txt</FilePath>
    <CaseSensitive>False</CaseSensitive>
  </Configuration>
</Extractor>
```

Content of the ToyotaVehicleList.txt file:

```
Yaris Hatchback
Yaris
Corolla
Matrix
Prius c
Prius
Prius Plug-in
Prius v
Camry
Camry Hybrid
Venza
Avalon
Sienna
RAV4
Highlander
Highlander Hybrid
FJ Cruiser
4Runner
Sequoia
Tacoma
Tundra
```

8.10.8.6.3.2 CESQueryMetadataExtractor

The CESQueryMetadataExtractor plugin adds the specified value to the specified metadata when the document matches the specified query.

Example: With the following CESQueryMetadataExtractor extractor definition, Potato will be extracted to the metadata Vegetables when the document matches the CES query potato AND (grow OR cook OR vegetable OR food).

```xml
<Extractor>
  <Impl>Coveo.TextAnalytics.Implementations.CESQueryMetadataExtractor, Coveo.TextAnalytics.Implementations</Impl>
  <Configuration>
    <Query>potato AND (grow OR cook OR vegetable OR food)</Query>
    <MetadataName>Vegetables</MetadataName>
    <MetadataValue>Potato</MetadataValue>
  </Configuration>
</Extractor>
```

Note: The CESQueryMetadataExtractor plugin generates one query to CES for each document and can therefore be slow when there are many documents.
8.10.8.6.3.3 MetadataAdderExtractor

The MetadataAdderExtractor plugin simply adds the specified value to the specified metadata for all documents.

Example: With the following MetadataAdderExtractor extractor definition, Potato will be added to the metadata Vegetables for all documents.

```xml
<Extractor>
  <Impl>Coveo.TextAnalytics.Implementations.MetadataAdderExtractor,
  Coveo.TextAnalytics.Implementations</Impl>
  <Configuration>
    <MetadataName>Vegetables</MetadataName>
    <MetadataValue>Potato</MetadataValue>
  </Configuration>
</Extractor>
```

8.10.8.6.3.4 RegexMetadataExtractor

This RegexMetadataExtractor plugin finds documents matching one specified regular expression and sets the value of the specified metadata name using one of following exclusive methods:

- By default, writes all found matches when neither the <MetadataValue> or <MetadataReplacement> parameters is defined.
- Optionally, when one or more <MetadataValue> parameter is defined, writes the specified value(s).
- Optionally, when one <MetadataReplacement> parameter is defined, writes the corresponding regular expression replacement value.

This extractor is generic and powerful, but can require significant CPU resources when specifying complex regular expressions.

Use the following parameters to define the extractor:

- `<Regex>`
  This required parameter specifies the regular expression (regex) that must be matched.

- `<MetadataName>`
  This required parameter specifies the name of the metadata to which a value is set when the content of a document matches the regular expression.

- `<MetadataValue>`
  One or more occurrences of this optional parameter specify one or more values to save in the metadata when the regular expression finds a match.

- `<MetadataReplacement>`
  This optional parameter specifies a regex replacement string used to create the metadata value from the content of regex matches in the document.
<CaseSensitive>

This optional parameter can be set to True to force the regular expression to be case sensitive. The default is False.

Examples: A document to analyze contains only: "I want to eat a potato".

With this content, for this document, the following extractor sets the Vegetables metadata to potato.

```xml
<Extractor>
  <Configuration>
    <MetadataName>Vegetables</MetadataName>
    <Regex>(potato|tuberosum)</Regex>
  </Configuration>
</Extractor>
```

With this content, for this document, the following extractor adds potato and tuberosum to the Vegetables metadata.

```xml
<Extractor>
  <Configuration>
    <MetadataName>Vegetables</MetadataName>
    <Regex>(potato|tuberosum)</Regex>
    <MetadataValue>potato</MetadataValue>
    <MetadataValue>tuberosum</MetadataValue>
  </Configuration>
</Extractor>
```

8.10.8.6.3.5 SalienceMetadataExtractor

The SalienceMetadataExtractor entity discovery plugin can extract one or more types of information (Themes, Named Entities, Sentiment).
Example: The following extractor processes up to 4096 characters of each document, extracts themes, named entities, and multi-level sentiment analysis.

```xml
<Extractor>
    <Impl>Coveo.TextAnalytics.Implementations.Salience.SalienceMetadataExtractor,
    Coveo.TextAnalytics.Implementations</Impl>
    <Configuration>
        <MaxDocLenToProcess>4096</MaxDocLenToProcess>
        <!-- Location of Salience files -->
        <SalienceLicensePath>E:\TXTAN\Lexalytics\license.v5</SalienceLicensePath>
        <SalienceDirectory>D:\TXTAN\Lexalytics\data</SalienceDirectory>
        <SalienceUserDirectory>D:\TXTAN\Lexalytics\user</SalienceUserDirectory>
        <!-- Types of information to extract -->
        <ExtractThemes>True</ExtractThemes>
        <!-- Sentiment analysis configuration -->
        <ExtractSentiment>True</ExtractSentiment>
        <PositiveThreshold>0.15</PositiveThreshold>
        <NegativeThreshold>-0.15</NegativeThreshold>
        <SentimentLevels>True</SentimentLevels>
        <SentimentLevelMultiple>2</SentimentLevelMultiple>
    </Configuration>
</Extractor>
```

Available parameters are:

**<MaxDocLenToProcess>**

The required MaxDocLenToProcess parameter defines the maximum number of characters from the content to send to the entity discovery plugin for each document. The recommended value is 4096. Assuming that on average English words contain 5 characters, 4096 characters correspond to about 800 words. A larger value can significantly increase the time required to process the run for many large documents.

**Note:** With a MaxDocLenToProcess set to 4096, smaller documents like emails are most likely fully processed. However, for longer documents containing thousands of word such as knowledge base articles, only the first 800 or so words will be processed.

**<SalienceLicensePath>**

This required parameter specifies the path and name of the Salience license file.

**<SalienceDirectory>**

This required parameter specifies the folder where Salience data files are located.

**<SalienceUserDirectory>**

This required parameter specifies the folder where Salience user data files are located.

**<ExtractThemes>**

Set this optional parameter to True to activate the extraction of themes, in which case you must also specify the <ThemeMetaName> global configuration parameter (see "<ThemeMetaName>" on page 711).

**<ExtractNamedEntities>**

Set this optional parameter to True to activate the extraction of predefined named entities. You cannot specify to the entity discovery plugin which named entities to extract. When you are only interested in a subset of named

www.coveo.com
entities, you can use a normalizer stage to remove unwanted named entity metadata (see "MetadataFilter" on page 722).

```xml
<ExtractSentiment>
  Set this optional parameter to True to activate the sentiment analysis, in which case you must also specify the
  <SentimentMetaName> global configuration parameter (see "<SentimentMetaName>" on page 711).
</ExtractSentiment>

```xml
<PositiveThreshold>
<NegativeThreshold>
  These parameters are required only when sentiment analysis is activated. The values are the level of sentiment
  score required to return a Positive or Negative sentiment. For an in between score, the returned sentiment is
  Neutral. Recommended values are respectively 0.15 and -0.15.
</NegativeThreshold>
</PositiveThreshold>

```xml
<SentimentLevels>
  Set this optional parameter to True to instruct the plugin to return multiple sentiment levels: Very Positive,
  Positive, Neutral, Negative, and Very Negative.
</SentimentLevels>

```xml
<SentimentLevelMultiple>
  When multiple sentiment level is activated, this parameter specifies the multiplier value applied to
  <PositiveThreshold> and <NegativeThreshold> values to determine the threshold score to respectively return
  Very Positive and Very Negative sentiment.

  **Example:** With the <PositiveThreshold>, <NegativeThreshold>, and <SentimentLevelMultiple> parameters respectively set to 0.15, -0.15, and 2, a document with a sentiment score greater than 0.30 returns a Very Positive sentiment. Similarly, a document with a sentiment score smaller than -0.30 returns a Very Negative sentiment.

  <VeryPositiveLabel>
<PositiveLabel>
<NeutralLabel>
<NegativeLabel>
<VeryNegativeLabel>

  You can use these optional parameters to change the default label for the sentiment levels.

  **Example:**

  ```xml
  <Extractor>
  <Impl>Coveo.TextAnalytics.Implementations.Salience.SalienceMetadataExtractor,
  Coveo.TextAnalytics.Implementations</Impl>
  <Configuration>
    ...
    <VeryPositiveLabel>Great!</VeryPositiveLabel>
    <PositiveLabel>Good!</PositiveLabel>
    <NeutralLabel>OK</NeutralLabel>
    <NegativeLabel>Not so good...</NegativeLabel>
    <VeryNegativeLabel>It's horrible!</VeryNegativeLabel>
    ...
  </Configuration>
  </Extractor>
  ```
8.10.8.6.4 Predefined Text Analytics Normalizers

You can use normalizer plugins in post-extraction stages to clean up metadata by either replacing or eliminating values to produce a more homogeneous set of metadata values.

8.10.8.6.4.1 MetadataBlackLister

The `MetadataBlackLister` plugin removes from a specified metadata, values that are defined in a blacklist in the form of a flat text file, one blacklist value per line.

**Example:** With the following normalizer definition, values from the `blacklist.txt` file found with the same capitalization in the metadata `Theme` are removed from the metadata.

```xml
<Normalizer>
  <Impl>Coveo.TextAnalytics.Implementations.MetadataBlackLister,
  Coveo.TextAnalytics.Implementations</Impl>
  <Configuration>
    <FilePath>D:\TextAnalytics\Config\BlackLists\blacklist.txt</FilePath>
    <CaseSensitive>True</CaseSensitive>
    <TypeRestriction>Theme</TypeRestriction>
  </Configuration>
</Normalizer>
```

8.10.8.6.4.2 MetadataRegexBlacklister

The `MetadataRegexBlacklister` plugin removes from a specified metadata, values that match at least one of the specified regular expressions. This normalizer is generic and powerful, but can require significant CPU resources when specifying complex regular expressions.

**Example:** With the following normalizer definition, sequences of numerical characters and strings starting with ‘`'` are removed from the `Theme` and `Place` metadata.

```xml
<Normalizer>
  <Impl>Coveo.TextAnalytics.Implementations.MetadataRegexBlacklister,
  Coveo.TextAnalytics.Implementations</Impl>
  <Configuration>
    <CaseSensitive>False</CaseSensitive>
    <TypeRestriction>Theme</TypeRestriction>
    <TypeRestriction>Place</TypeRestriction>
    <Regex>^[0-9]+$</Regex>
    <Regex>'^.*$</Regex>
  </Configuration>
</Normalizer>
```

8.10.8.6.4.3 MetadataFilter

When you use the `SalienceMetadataExtractor` entity discovery plugin, it extracts named entities for all categories it knows (see "SalienceMetadataExtractor" on page 719). You can use the `MetadataFilter` plugin to eliminate metadata for specific unwanted named entity categories.

www.coveo.com
Examples:

With the following normalizer definition, only the Person, Company, and Place metadata are kept.

```xml
<Normalizer>
    <Impl>Coveo.TextAnalytics.Implementations.MetadataFilter,
    Coveo.TextAnalytics.Implementations</Impl>
    <Configuration>
        <InverseMode>True</InverseMode>
        <FilteredName>Company</FilteredName>
        <FilteredName>Person</FilteredName>
        <FilteredName>Place</FilteredName>
    </Configuration>
</Normalizer>
```

With the following normalizer definition, only the Person metadata are removed, all other named entity metadata are kept.

```xml
<Normalizer>
    <Impl>Coveo.TextAnalytics.Implementations.MetadataFilter,
    Coveo.TextAnalytics.Implementations</Impl>
    <Configuration>
        <InverseMode>False</InverseMode>
        <FilteredName>Person</FilteredName>
    </Configuration>
</Normalizer>
```

8.10.8.6.4.4 MetadataNormalizer

The MetadataNormalizer plugin loads one specified text file or all text files found in the specified folder. The text files must contain tab separated expressions. The first column contains a unique expression to look for. The second column contains the replacement expression, or expressions separated by a semi-colon (;). You can restrict the normalization to one or more metadata names, otherwise the metadata value normalization from all files applies to all metadata.

**Tip:** In a pipeline, you can use more than one MetadataNormalizer instance, typically each applying the content of one normalization file to one metadata.
Example: With the following normalizer definition, the plugin loads the normalization expression pairs from the D:\TXTAN\Config\Normalizations\PeopleNameNormalization.txt file.

```xml
<Normalizer>
  <Impl>Coveo.TextAnalytics.Implementations.MetadataNormalizer,
  Coveo.TextAnalytics.Implementations</Impl>
  <Configuration>
    <FilePath>D:\TXTAN\Config\Normalizations\PeopleNameNormalization.txt</FilePath>
    <CaseSensitive>False</CaseSensitive>
    <TypeRestriction>People</TypeRestriction>
  </Configuration>
</Normalizer>
```

When the file contains the following lines:

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>RKennedy</td>
<td>Robert F. Kennedy</td>
</tr>
<tr>
<td>R. Kennedy</td>
<td>Robert F. Kennedy</td>
</tr>
<tr>
<td>Bob Kennedy</td>
<td>Robert F. Kennedy</td>
</tr>
<tr>
<td>B. Obama</td>
<td>Barack Obama;President</td>
</tr>
</tbody>
</table>

When found in the People metadata, Robert Kennedy's specified name variants are replaced by Robert F. Kennedy. When B. Obama is found, it is replaced by two values: Barack Obama and President.

8.10.8.6.5 Predefined Text Analytics Outputters

One outputter stage completes the text analytics pipeline by sending the extracted information to the desired output.

**Note:** You can create a pipeline with no outputter stage to review logs of the process without saving to results.

8.10.8.6.5.1 CESITaggerOutputter

The CESITaggerOutputter plugin is the module used to save the result of the text analytics pipeline back in the Coveo unified index using the tagging mechanism. This outputter saves metadata values extracted by the text analytics pipeline for processed documents in tag fields. When it does not already exist in the index, a tag field is automatically created and named by concatenating the specified prefix with the metadata name. You can optionally clear all or specified tag fields to ensure the output of the current pipeline replaces existing values rather than be appended to existing values.
Example: With the following outputter definition, in the Coveo unified index, the values of the @txtantheme, @txtancompany, @txtanperson, and @txtanplace tag fields are cleared for all processed documents and the metadata extracted by this pipeline is associated to processed documents in the corresponding tag fields.

```xml
<Outputter>
  <Impl>Coveo.TextAnalytics.Implementations.CESITaggerOutputter, Coveo.TextAnalytics.Implementations</Impl>
  <Configuration>
    <TagNamePrefix>@TXTAN</TagNamePrefix>
    <ClearAllTextAnalyticsTags>False</ClearAllTextAnalyticsTags>
    <ClearTagField>@txtantheme</ClearTagField>
    <ClearTagField>@txtancompany</ClearTagField>
    <ClearTagField>@txtanperson</ClearTagField>
    <ClearTagField>@txtanplace</ClearTagField>
  </Configuration>
</Outputter>
```

Available parameters are:

- `<TagNamePrefix>`
  This required parameter specifies the prefix concatenated to the metadata names to build tag field names. The prefix can only include alphanumerical characters.

  Example: With `<TagNamePrefix>@TXTAN</TagNamePrefix>`, Theme metadata values are injected in the unified index in the @txtantheme tag field.

- `<ClearAllTextAnalyticsTags>`
  Set this optional parameter to True to delete all values from tag fields for which the name starts with the prefix specified in the `<TagNamePrefix>` parameter. The default value is False.

  Important: Be careful, the `<ClearAllTextAnalyticsTags>` parameter will delete values created by other runs and jobs for tag fields which names start with the value specified in the `<TagNamePrefix>` parameter.

  Example: When you have a first run with the `<TagNamePrefix>` parameter set to TXTAN2 and a second run in which it is set to TXTAN, because TXTAN is a subset of TXTAN2, setting `<ClearAllTextAnalyticsTags>` to True on the second run deletes tag field values produced by the first run!

- `<ClearTagField>`
  This optional parameter clears the values of the specified tag field. You can specify multiple instances of this parameter.

- `<TagFieldCreatorName>`
- `<TagFieldCreatorPassword>`
  These required parameters contain the username and password of a user that has permissions to create tag fields in the Coveo unified index.
Note: These parameters will be automatically filled with default values (encrypted for the password) when creating your pipeline configuration files from TAnGO using a template (see "Creating a Custom Run or Job from a Template" on page 707).

<TagFieldCreatorSecurityProvider>
This optional parameter specifies the security provider where the user specified in <TagFieldCreatorName> parameter is defined. The default value is Active Directory.

<TagFieldSIDName>
This optional parameter specifies the tag field security ID (SID) to use to specify who has the permissions to see the content of this tag field. This parameter allows you to restrict access to the content of a tag field to a specific user or group of users. The default value is S-1-1-0 (Everyone).

<TagFieldSIDType>
This optional parameter specifies the tag field security ID (SID) type to use to specify who has the permissions to see the content of this tag field. The default value is Unknown because everyone is the default <TagFieldSIDName> value. Other valid values are User and Group.

<TagFieldSIDSecurityProvider>
This optional parameter specifies the security provider where the security ID (SID) specified in the <TagFieldSIDName> parameter is defined. The default value is Active Directory.

Note: A run will stop if the CESITaggerOutputter plugin encounters a document that cannot be tagged in the Coveo unified index. This can happen when the index becomes in read-only mode. A continuous run will restart at the specified time interval and restart where it left whenever the index is back in read-write mode.

8.10.8.6.5.2 FSDumpMetadataPrinter
The FSDumpMetadataPrinter plugin saves extracted metadata to a specified comma-separated value (CSV) text file. A line is created in the file for each extracted metadata value and is in the following format:

[DocumentID] [DocumentTitle] [MetadataName] [ExtractedMetadataValue]

This outputter is typically useful for pipeline debugging and fine-tuning purposes. You can inspect the file to review the exact output of the pipeline, identifying problems as well as unwanted or missing output values.

Example: With the following outputter definition, the extracted values Theme, Company, and Person metadata are saved to the C:\Temp\Debug-AllMetadata.csv file.

<Outputter>
  <Impl>Coveo.TextAnalytics.Implementations.FSDumpMetadataPrinter</Impl>
  <Configuration>
    <DirectoryPath>C:\Temp\</DirectoryPath>
    <Prefix>Debug</Prefix>
    <WantedField>Theme</WantedField>
    <WantedField>Company</WantedField>
    <WantedField>Person</WantedField>
  </Configuration>
</Outputter>
Available parameters:

<DirectoryPath>

This required parameter specifies the folder where the CSV file is saved.

<Prefix>

This required parameter specifies the prefix of the CSV file name, completed with -AllMetadata.csv.

<WantedField>

At least one instance of this parameter is required to specify metadata for which values will be outputted. Use one instance of this parameter per metadata that you want to output.

8.10.8.6.5.3 FSDumpResultProcessor

The FSDumpResultProcessor plugin creates one text file per fetched document. The files only contain the fetched content of the document, not original or extracted metadata. The files are saved in a specified folder with a name of the form [DocID].txt where [DocID] is the value of the @sysrowid field of the document when the CESIQuerierFetcher fetcher is used. Otherwise, the [DocID] is that set by the fetcher used to retrieve documents. This outputter is typically useful for pipeline debugging to validate the content that is extracted by the fetcher.

Example: With the following outputter definition, the fetched text content of each processed document is saved in the C:\Temp\ folder in a file named after its [DocID].

```xml
<Outputter>
  <Impl>Coveo.TextAnalytics.Implementations.FSDumpResultProcessor,
  Coveo.TextAnalytics.Implementations</Impl>
  <Configuration>
    <DirectoryPath>C:\Temp\</DirectoryPath>
  </Configuration>
</Outputter>
```

8.10.8.7 Predefined Text Analytics Job Plugins

A job simply runs a piece of code. It does not work on a set of documents like a run does. The piece of code associated with many of the following predefined text analytics job plugins take advantage of the Coveo tagging mechanism to allow often efficient batch operations on text analytics tag fields.

8.10.8.7.1 CreateTagField

The CreateTagField plugin creates specified tag fields in the index. Unlike the outputter of runs, jobs cannot automatically create the tag fields corresponding to extracted metadata names as they are not part of a document pipeline. You must therefore run this job plugin to create necessary tag fields before running job plugins that save metadata values in these tag fields.
Example: The following job definition creates the @txtanexample1 and @txtanexample2 tag fields.

```xml
<Job Name="CreateTagFieldExample">
  <Impl>Coveo.TextAnalytics.Implementations.CreateTagFieldJob,
  Coveo.TextAnalytics.Implementations</Impl>
  <Configuration>
    <CreateTagField>@txtanexample1</CreateTagField>
    <CreateTagField>@txtanexample2</CreateTagField>
    <!-- Create runs from templates using TAnGO to automatically fill the following parameters with default values -->
    <TagFieldCreatorName>MyDomain\MyTextAnalyticsAccount</TagFieldCreatorName>
    <TagFieldCreatorPassword Encrypted="True">bQxhRBprySuC4UZcDzE3Dw==</TagFieldCreatorPassword>
  </Configuration>
</Job>
```

8.10.8.7.2 ClearFieldJob

The `ClearFieldJob` plugin internally lists all values found in a tag field, and then uses one tagging query for each value to clear the values of a specific tag field for indexed documents returned by a specified query. This plugin is available in Text Analytics version 2.0.11+.

**Note:** When the number of available tag field values is large, building the list can take minutes during which nothing appears in the Job logs. Then, the tagging queries for each value start appearing in the job logs, progressively clearing the tag field values in the index.

Example: With the following job definition, the values for the @txtantheme tag field are deleted for all indexed documents returned by the @syslanguage=English query.

```xml
<Job Name="ClearFieldJob">
  <Configuration>
    <TagField>@txtantheme</TagField>
    <ScopeQuery>@syslanguage=English</ScopeQuery>
  </Configuration>
</Job>
```

8.10.8.7.3 MasterFieldMoverJob

The `MasterFieldMoverJob` plugin creates a new tag field containing the most frequent values from another tag field. The goal of this migration is to create a top list from a long list of values and assign the top list tag field to a facet rather than the original one to prevent long facet loading. This plugin is available in Text Analytics version 2.0.11+.
**Example:** Several million themes were extracted from a document set. With the following job definition, the `@txtanmastertheme` tag field is created and will contain the 10,000 most frequent themes found in the `@txtantheme` tag field.

```xml
<Job Name="MasterFieldMoverJob">
  <Impl>Coveo.TextAnalytics.Implementations.MasterFieldMoverJob,
  Coveo.TextAnalytics.Implementations</Impl>
  <Configuration>
    <Name>MasterFieldMoverJob</Name>
    <TagFieldCreatorName></TagFieldCreatorName>
    <TagFieldCreatorPassword Encrypted="True"></TagFieldCreatorPassword>
    <TagField>@txtantheme</TagField>
    <MasterTagField>@txtanmastertheme</MasterTagField>
    <MasterListSize>10000</MasterListSize>
  </Configuration>
</Job>
```

### 8.10.8.7.4 BlacklistJob

The **BlacklistJob** plugin uses tagging queries to remove blacklisted values defined in a specified flat text file from one or more specified tag fields for indexed documents returned by a specified query.

The format of the file containing the blacklisted expressions is the same as the one for the **MetadataBlacklister** normalizer used in run stages so you can share the file between them (see "MetadataBlackLister" on page 722).

**Example:** With the following job definition, the **BlacklistJob** plugin removes values defined in the `D:\TextAnalytics\Config\normalizations\blacklist-example.txt` file that are found in the `@txtantheme` and `@txtanplace` tag fields for indexed documents returned by the `@uri="gov"` query.

```xml
<Job Name="BlacklistJobExample">
  <Impl>Coveo.TextAnalytics.Implementations.BlacklistJob,
  Coveo.TextAnalytics.Implementations</Impl>
  <Configuration>
    <Name>BlacklistJobExample</Name>
    <TagField>@TXTANTheme</TagField>
    <TagField>@TXTANPlace</TagField>
    <ScopeQuery>@uri="gov"</ScopeQuery>
    <FilePath>D:\TextAnalytics\Config\normalizations\blacklist-example.txt</FilePath>
  </Configuration>
</Job>
```

### 8.10.8.7.5 NormalizationJob

The **NormalizationJob** plugin uses tagging queries to normalize values in one or more specified tag fields as defined in a specified flat text file for indexed documents returned by a specified query.

The format of the file containing the normalization values is the same as the one for the **MetadataNormalizer** normalizer used in run stages so you can share the file between them (see "MetadataNormalizer" on page 723).
Example: With the following job definition, the NormalizationJob plugin homogenizes values found in the @txtantheme tag field using normalized values defined in the D:\TextAnalytics\Config\normalizations\normalization-example.txt file for English indexed documents returned by the @syslanguage=English query.

```xml
<Job Name="TestNormalizerJob">
  <Configuration>
    <Name>TestNormalizerJob</Name>
    <TagField>@TXTANTheme</TagField>
    <ScopeQuery>@syslanguage=English</ScopeQuery>
    <FilePath>D:\TextAnalytics\Config\normalizations\normalization-example.txt</FilePath>
  </Configuration>
</Job>
```

8.10.8.7.6 WhitelistBasicMatcherJob

The WhitelistBasicMatcherJob plugin uses tagging queries to add values defined in a specified flat text file to a specified tag field when found in indexed documents returned by a specified query.

The format of the whitelist file is the same as the one for the Whitelister plugin used in run stages so you can share the file between them (see "Whitelister" on page 716).

Example: With the following job definition, the WhitelistBasicMatcherJob plugin adds values defined in the D:\TextAnalytics\Config\whitelists\wizards-example.txt file to the @txtantheme tag field when found in indexed documents returned by the @syslanguage=English query.

```xml
<Job Name="TestWhitelistBasicMatcherJob">
  <Configuration>
    <Name>TestWhitelistBasicMatcherJob</Name>
    <TagField>@TXTANTheme</TagField>
    <ScopeQuery>@syslanguage=English</ScopeQuery>
    <FilePath>D:\TextAnalytics\Config\whitelists\wizards-example.txt</FilePath>
  </Configuration>
</Job>
```

8.10.8.7.7 WhitelistQueryMatcherJob

The WhitelistQueryMatcherJob plugin reads a flat text file that specifies one or more queries and a corresponding tagging values. The plugin evaluates returned indexed documents against the queries, and when there is a match, adds the corresponding value to the specified tag field.
Example: With the following job definition, the WhitelistQueryMatcherJob plugin reads the query-based-job-example.txt file. When a document contains either of the following words: cucurbita, squash, pumpkin, courgette, fruits is added to the @txtantheme tag field.

```xml
<Job Name="TestWhitelistQueryMatcherJob">
  <Configuration>
    <Name>TestWhitelistQueryMatcherJob</Name>
    <TagField>@TXTANTheme</TagField>
    <ScopeQuery>@syslanguage=English</ScopeQuery>
    <FilePath>D:\TextAnalytics\Config\whitelists\query-based-job-example.txt</FilePath>
  </Configuration>
</Job>
```

The query-based-job-example.txt contains:

cucurbita OR squash OR pumpkin OR courgette fruits

The file can contain one or more queries. Each query is on one line followed by a tab delimited tag field value. The file format is not compatible with any module used for runs.

Note: The expression in the first column of the file is used as is for the query and must therefore be a complete and valid query, including double-quote characters when needed.

8.10.9 Clearing Text Analytics Tag Fields

At some point in the development of your text analytics implementation, you may need to clear all or some of the tag fields set by previous text analytics jobs or runs.

To clear text analytics tags fields

- When you only want to clear specific known tag field values:
  1. Create a text file containing the list of values to clear.
  2. Use the BlacklistJob plugin to clear the tags (see "BlacklistJob" on page 729).

- When you want to clear all values of all tags or specified tags, you have two options:

  Note: Regarding performance, when the number of documents to process is large and the number of unique tag field values is small, using a job is faster. On the opposite, when the number of documents is small and the number of tag field values is large, using a run is more efficient.

  - Option 1 - Using a run
    1. Create a new run that processes all documents for which you want the tag fields to be cleared. For this run, you only need CES fetcher and outputter plugins (see "CESIQuerierFetcher" on page 713 and "CESITaggerOutputter" on page 724).

    Tip: You can also reprocess all documents with an existing run (see "Reprocessing All Documents with a Text Analytics Run" on page 732).
2. In the XML definition of the CESITaggerOutputter plugin, either set the `<ClearAllTextAnalyticsTags>` parameter to `True`, or specify each field to clear using the `<ClearTagField>` parameter.

- Option 2 - Using a job

Use the `ClearFieldJob` plugin to remove all values of specified tag fields for documents returned by the specified query (see "ClearFieldJob" on page 728).

8.10.10 Reprocessing All Documents with a Text Analytics Run

Sometimes, you may need to restart a text analytics run from scratch, reprocessing all documents. The Text Analytics module keeps track of which document was last processed by each registered run that was executed at least once. This information is stored in a cookie file (`[Run_Name].state`), one per registered run, in the `[Text_Analytics_Path]\State\` folder. The cookie file only contains the `@sysrowid` field value of the last document processed by the run.

To reprocess all documents from scratch

1. Start TAnGO (see "Starting TAnGO" on page 694).

2. Ensure that the run for which you want to reprocess all documents is registered, and then select it in the top-left panel.

3. In the Job Details panel, on the line for the State parameter, click the reset icon to clear the `@sysrowid` field value, forcing the run to reprocess all documents.
4. On the toolbar, click **Run** to launch the run.
9. Coveo Platform Connectors

The Coveo Platform includes a selection of connectors allowing you to index content from a variety of third-party repositories. The connectors are made available through your Coveo license. You can view the allowed connector sources for your current Coveo license using the Administration Tool (see "What Information Is Displayed in the License Page?" on page 525).

Notes:

- Contact the Coveo Sales when you want to add a connector to your license. Contact the Coveo Professional Services when you want to develop connectors for other repositories.
- Refer to the list of connectors available with Coveo for Salesforce.

The following table lists the connectors available with the Coveo Platform 7.

<table>
<thead>
<tr>
<th>Logo</th>
<th>Available connector</th>
<th>Supported repository versions</th>
<th>No longer supported versions</th>
<th>Repository type</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="logo.png" alt="Aha! Logo" /></td>
<td>Aha!</td>
<td>N/A</td>
<td>3.3, 3.4</td>
<td>Product Management</td>
</tr>
<tr>
<td><img src="logo.png" alt="Alfresco One Logo" /></td>
<td>Alfresco One</td>
<td>4 to 4.2.5</td>
<td>3.3, 3.4</td>
<td>Enterprise Content Management (ECM)</td>
</tr>
<tr>
<td><img src="logo.png" alt="Amazon S3 Logo" /></td>
<td>Amazon S3</td>
<td>N/A</td>
<td></td>
<td>File storage</td>
</tr>
<tr>
<td><img src="logo.png" alt="Atlassian Confluence (Legacy) Logo" /></td>
<td>Atlassian Confluence (Legacy) Deprecated</td>
<td>5.5 to 5.8.5 Cloud</td>
<td>2.5.3, 3.x, 4.x, 5.4</td>
<td>Wiki</td>
</tr>
<tr>
<td><img src="logo.png" alt="Atlassian Confluence V2 Logo" /></td>
<td>Atlassian Confluence V2</td>
<td>6.7 to 7.1 Cloud</td>
<td>5.7 to 6.6</td>
<td>Wiki</td>
</tr>
<tr>
<td><img src="logo.png" alt="Atlassian Jira Software Logo" /></td>
<td>Atlassian Jira Software</td>
<td>6.1 to 7.1.2 Cloud</td>
<td>5.2 to 6.0</td>
<td>Issue and Bug Tracker</td>
</tr>
<tr>
<td>Logo</td>
<td>Available connector</td>
<td>Supported repository versions</td>
<td>No longer supported versions</td>
<td>Repository type</td>
</tr>
<tr>
<td>------------</td>
<td>---------------------</td>
<td>------------------------------</td>
<td>------------------------------</td>
<td>-----------------------------</td>
</tr>
<tr>
<td>Basecamp</td>
<td>N/A</td>
<td></td>
<td></td>
<td>Project Management</td>
</tr>
<tr>
<td>Box</td>
<td>N/A</td>
<td></td>
<td></td>
<td>File storage</td>
</tr>
<tr>
<td>Database</td>
<td>N/A</td>
<td></td>
<td></td>
<td>Database</td>
</tr>
<tr>
<td>Desktop</td>
<td>N/A</td>
<td></td>
<td></td>
<td>File/PST</td>
</tr>
<tr>
<td>Dropbox for Business</td>
<td>N/A</td>
<td></td>
<td></td>
<td>File storage</td>
</tr>
<tr>
<td>Ektron CMS</td>
<td>8.0 (Prototype)</td>
<td></td>
<td></td>
<td>WCM</td>
</tr>
<tr>
<td>Deprecated</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>EMC Documentum</td>
<td>7.0</td>
<td>5.3 to 6.7</td>
<td></td>
<td>Enterprise Content Management (ECM)</td>
</tr>
<tr>
<td>Episerver CMS</td>
<td>6 (Beta)</td>
<td></td>
<td></td>
<td>Web Content Management System (WCMS)</td>
</tr>
<tr>
<td>Deprecated</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Files</td>
<td>N/A</td>
<td></td>
<td></td>
<td>File/PST files</td>
</tr>
<tr>
<td>(Microsoft Windows, Samba)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Logo</td>
<td>Available connector</td>
<td>Supported repository versions</td>
<td>No longer supported versions</td>
<td>Repository type</td>
</tr>
<tr>
<td>------</td>
<td>---------------------</td>
<td>------------------------------</td>
<td>-----------------------------</td>
<td>----------------</td>
</tr>
<tr>
<td><img src="image1" alt="Logo" /></td>
<td>Google Drive Compact for Work</td>
<td>N/A</td>
<td></td>
<td>File storage</td>
</tr>
<tr>
<td><img src="image2" alt="Logo" /></td>
<td>Google Drive for Work</td>
<td>N/A</td>
<td></td>
<td>File storage</td>
</tr>
<tr>
<td><img src="image3" alt="Logo" /></td>
<td>Google Sites</td>
<td>N/A (Beta)</td>
<td></td>
<td>WCM</td>
</tr>
<tr>
<td><img src="image4" alt="Logo" /></td>
<td>Gmail for Work</td>
<td>N/A (Beta)</td>
<td></td>
<td>Email</td>
</tr>
<tr>
<td><img src="image5" alt="Logo" /></td>
<td>IEM Lotus Notes Deprecated</td>
<td>8.5.1</td>
<td>7, 8</td>
<td>Email</td>
</tr>
<tr>
<td><img src="image6" alt="Logo" /></td>
<td>IEM WebSphere (Lotus Web Content Management) Deprecated</td>
<td>8.0</td>
<td>6.0, 6.1.5</td>
<td>Web Content Management System (WCMS)</td>
</tr>
<tr>
<td><img src="image7" alt="Logo" /></td>
<td>Jive Jive 5 / Clearspace / S3S Deprecated</td>
<td>2.5.5, 2.5.7, 3.0, 4.0, 4.5, 5.0</td>
<td></td>
<td>Collaboration</td>
</tr>
<tr>
<td><img src="image8" alt="Logo" /></td>
<td>LDAP (Lightweight Directory Access Protocol)</td>
<td>N/A</td>
<td></td>
<td>Directory information</td>
</tr>
<tr>
<td><img src="image9" alt="Logo" /></td>
<td>Liferay</td>
<td>6 (Beta)</td>
<td></td>
<td>Collaboration</td>
</tr>
<tr>
<td><img src="image10" alt="Logo" /></td>
<td>Lithium</td>
<td>N/A</td>
<td></td>
<td>Social customer experience management</td>
</tr>
<tr>
<td>Logo</td>
<td>Available connector</td>
<td>Supported repository versions</td>
<td>No longer supported versions</td>
<td>Repository type</td>
</tr>
<tr>
<td>------</td>
<td>---------------------</td>
<td>-------------------------------</td>
<td>-----------------------------</td>
<td>-----------------</td>
</tr>
<tr>
<td><img src="image" alt="Microsoft Active Directory" /></td>
<td>Microsoft Active Directory</td>
<td>N/A</td>
<td></td>
<td>Security</td>
</tr>
<tr>
<td><img src="image" alt="Microsoft Dynamics" /></td>
<td>Microsoft Dynamics</td>
<td>2013 and 2015 On-Premises, and Online</td>
<td></td>
<td>Customer Relationship Management (CRM)</td>
</tr>
<tr>
<td><img src="image" alt="Microsoft Exchange" /></td>
<td>Microsoft Exchange</td>
<td>2010, 2013, 2016 (on-premises and hybrid deployment) Online</td>
<td>2003, 2007</td>
<td>Email</td>
</tr>
<tr>
<td><img src="image" alt="Microsoft OneDrive for Business" /></td>
<td>Microsoft OneDrive for Business</td>
<td>N/A</td>
<td></td>
<td>File storage</td>
</tr>
<tr>
<td><img src="image" alt="Microsoft SharePoint" /></td>
<td>Microsoft SharePoint</td>
<td>2010, 2013, 2016 Online</td>
<td>MOSS 2007</td>
<td>Collaboration</td>
</tr>
<tr>
<td><img src="image" alt="Microsoft SharePoint (Legacy) Deprecated" /></td>
<td>Microsoft SharePoint (Legacy) Deprecated</td>
<td>2010, 2013 Online</td>
<td>WSS 3, MOSS 2007</td>
<td>Collaboration</td>
</tr>
<tr>
<td><img src="image" alt="OpenText Content Server (formerly Livelink)" /></td>
<td>OpenText Content Server (formerly Livelink)</td>
<td>16 and 16.2</td>
<td>9.7.1, 10, 10.5</td>
<td>Enterprise Content Management (ECM)</td>
</tr>
<tr>
<td><img src="image" alt="Oracle Knowledge (formerly InQuira)" /></td>
<td>Oracle Knowledge (formerly InQuira)</td>
<td>8.4.2.2 to 8.5.1</td>
<td></td>
<td>Customer Relationship Management (CRM)</td>
</tr>
<tr>
<td><img src="image" alt="Oracle UCM (formerly Stellent)" /></td>
<td>Oracle UCM (formerly Stellent)</td>
<td>10r3, 11g</td>
<td></td>
<td>Enterprise Content Management (ECM)</td>
</tr>
<tr>
<td><img src="image" alt="PTC Windchill" /></td>
<td>PTC Windchill</td>
<td>10.1 (M010 and M040)</td>
<td></td>
<td>Product Lifecycle Management</td>
</tr>
<tr>
<td>Logo</td>
<td>Available connector</td>
<td>Supported repository versions</td>
<td>No longer supported versions</td>
<td>Repository type</td>
</tr>
<tr>
<td>--------------</td>
<td>---------------------</td>
<td>-------------------------------</td>
<td>-----------------------------</td>
<td>-----------------------</td>
</tr>
<tr>
<td><img src="image" alt="RSS Logo" /></td>
<td>RSS</td>
<td>RSS 1.0, 2.0, Atom 1.0</td>
<td></td>
<td>RSS feed</td>
</tr>
<tr>
<td><img src="image" alt="Salesforce Logo" /></td>
<td>Salesforce</td>
<td>API 30, API 32, API 33, API 34</td>
<td></td>
<td>Customer Relationship Management (CRM)</td>
</tr>
<tr>
<td><img src="image" alt="Sitecore Logo" /></td>
<td>Queue (Sitecore)</td>
<td>see Supported Sitecore Versions and Dependencies</td>
<td></td>
<td>Web Content Management System (WCMS)</td>
</tr>
<tr>
<td><img src="image" alt="Sitecore Logo" /></td>
<td>Sitecore</td>
<td>6.0 to 6.6, 7.0 to 7.2</td>
<td></td>
<td>Web</td>
</tr>
<tr>
<td><img src="image" alt="Sitecore Logo" /></td>
<td>Sitecore (Legacy)</td>
<td>5.3, 6.0 to 6.5</td>
<td></td>
<td>Web</td>
</tr>
<tr>
<td><img src="image" alt="Sitecore Logo" /></td>
<td>Sitemap</td>
<td>N/A</td>
<td></td>
<td>Web</td>
</tr>
<tr>
<td><img src="image" alt="Symantec Logo" /></td>
<td>Symantec Enterprise Vault (formerly KVS)</td>
<td>10, 11, 12</td>
<td>7, 8, 9</td>
<td>Archiving</td>
</tr>
<tr>
<td><img src="image" alt="TargetProcess Logo" /></td>
<td>TargetProcess</td>
<td>3</td>
<td></td>
<td>Issue tracking</td>
</tr>
<tr>
<td><img src="image" alt="Twitter Logo" /></td>
<td>Twitter v2</td>
<td>N/A (Beta)</td>
<td></td>
<td>Social media</td>
</tr>
<tr>
<td><img src="image" alt="Web Pages Logo" /></td>
<td>Web Pages</td>
<td>N/A</td>
<td></td>
<td>Web</td>
</tr>
<tr>
<td><img src="image" alt="Yammer Logo" /></td>
<td>Yammer</td>
<td>NA</td>
<td></td>
<td>Social media</td>
</tr>
</tbody>
</table>
9.1 What Does Deprecated Mean for a Coveo Connector?

Coveo continuously improves existing connectors and creates new ones, but also deprecates the old ones or drops support for repository versions entering their end-of-life.

9.1.1 Connector Deprecation

Older Coveo CES 7.0 connectors (mostly legacy ones) are progressively put in the **Deprecated** state, typically after a newer and more capable connector as been made available for a while to better or exclusively support the latest repository versions using the latest API versions. Deprecated connectors often allow to index repository end-of-life versions generally no longer supported by the software vendor themselves.

Basically, a deprecated connector is generally still usable, but is:

- No longer enhanced (no new features)
- Minimally maintained
- No longer tested, consequently there is no guarantee it will work without issues
- Planned to be removed (obsolete) from CES in the future

**Note**: You are going to be notified well ahead of time before these connectors are removed from CES. If a second-generation of these connectors is available, it is highly recommended to migrate to the new version as soon as possible to benefit from bug fixes, new features, support of new repository versions, etc.

The following table lists the deprecated connectors and additional information.
## 9.1.2 Repository Version Support Deprecation

Coveo connectors only support repository versions that are actively maintained by their software vendor. When a repository version is marked as end-of-life by its vendor, Coveo will drop the active connector support for that specific repository version.

A connector is generally still usable with a repository version for which the support is deprecated, however:

- Coveo no longer actively maintains and tests the connector for that particular version.
- If any additional work is required, it will be done through a specific engagement with Coveo Professional Services.

The connector documentation identifies repository versions for which the support is deprecated (see the No longer supported column in the table of "Coveo Platform Connectors" on page 734).

### 9.2 Aha! Connector

**CES 7.0.7711+ (December 2014)**
Aha! provides Web-based product management tools and roadmapping software for agile product managers (see www.aha.io). The Coveo connector for Aha! allows Coveo administrators to index and integrate the Aha! content into the Coveo unified index and make it easily searchable by end-users.

The connector indexes the permissions on Product lines and Products so that in the Coveo search interfaces, an authenticated user can easily find any but only content to which he has access in the Aha! user interface.

9.2.1 Features

The Aha! connector features are:

**Content indexing**

The connector can retrieve and index exclusively the following Aha! content type:

- Product line
- Product
- Idea
- Feature
- Release
- Requirement
- Task
- Comment
- Attachment

9.2.2 Limitation

- Incremental refresh is not supported.

**Feature History**

<table>
<thead>
<tr>
<th>CES version</th>
<th>Monthly release</th>
<th>Features</th>
</tr>
</thead>
<tbody>
<tr>
<td>7.0.7338</td>
<td>January 2015</td>
<td>Adding default mapping file, field set, and JavaScript Search UI.</td>
</tr>
<tr>
<td>7.0.7711</td>
<td>December 2014</td>
<td>Connector introduction</td>
</tr>
</tbody>
</table>

**What's Next?**

Review the steps to deploy the Aha! connector (see "Aha! Connector Deployment Overview" on page 742).
9.2.3 Aha! Connector Deployment Overview

The following procedure outlines the steps needed to deploy the Aha! connector. The steps indicate the order in which you must perform configuration tasks on the Coveo server.

To deploy the Aha! connector

1. Validate that your environment meets the requirements (see "Aha! Connector Requirements" on page 742).
2. In Aha!, create and register an OAuth2 application to get an access token to be used by the Coveo connector (see "Granting the Connector Access to Your Aha! Content" on page 742).
3. On the Coveo server, in the Coveo Administration Tool:
   a. CES 7.0.7338+ (January 2015) Create an Aha! field set to take advantage of the available Aha! metadata.
      i. It is recommended to start by importing the default Aha! field set file ([[CES_Path]\Bin\Coveo.CES.CustomCrawlers.Aha.FieldSet.xml] to create fields for all the metadata available by default from the Aha! content.
      ii. When you created custom metadata for your Aha! content, add corresponding fields to the field set.
   b. Configure and index an Aha! source.

The connector must know how to access your Aha! content to be able to index it (see "Configuring and Indexing a Aha! Source" on page 744).

9.2.4 Aha! Connector Requirements

Your environment must meet the following requirements to be able to use the Aha! connector:

- CES 7.0.7256+ (December 2014)
  The connector was introduced with the CES 7.0.7256 December 2014 release.
- Coveo license for the Aha! connector
  Your Coveo license must include support for the Aha! connector to be able to use this connector.

What's Next?

Get an access token to be used by the connector to gain access to your Aha! content (see "Granting the Connector Access to Your Aha! Content" on page 742).

9.2.5 Granting the Connector Access to Your Aha! Content

The Coveo Aha! connector needs an OAuth2 access token to gain access to and index your Aha! content. This is done from the Aha! web site by creating and registering an OAuth application and then get an OAuth access token (see the Aha! document OAuth2 Authentication).

To grant the connector access to your Aha! content

1. Using an Aha! account that has read permissions on all the items that you want to index, connect to Aha! ([YourDomain].aha.io).
2. Access the applications page to create and register your application:
   a. Under Oauth applications you have created, click register a new application.
   b. In the Name box, enter an application name that indicates its purpose, such as Coveo Connector.
   c. In the Redirect uri box, enter urn:ietf:wg:oauth:2.0:oob to be able to receive and view the access token value directly in your browser address bar in step 6.
   d. Click Save.

3. In the Application: [YourAppName] page, copy the URL from the Authorize URL parameter.

   ![Application: Coveo Connector](https://secure.aha.io/oauth/authorize?client_id=649618e7c325ae57119a4324705cbd)

4. In a browser, paste the copied URL in the address box, and press enter.

5. In the Authorize Coveo Connector to use your account? page that appears, click Authorize.
6. In the next browser page displaying a JSON output returned by Aha!, in the browser address box, copy the access token value (string after ?access_token=).

Example: In your browser address box, the URL looks like the following image. Copy the highlighted part, the access token value.

What's Next?

Create a Aha! source that will use the access token obtained in the above procedure (see "Configuring and Indexing a Aha! Source" on page 744).

9.2.6 Configuring and Indexing a Aha! Source

A source defines a set of configuration parameters for indexing the content of a specific Aha! account.

To configure and index an Aha! source

1. On the Coveo server, access the Administration Tool.

2. Select Index > Sources and Collections.

3. In the Collections section:
a. Select an existing collection in which you want to add the new source.

OR

b. Click Add to create a new collection.

4. In the Sources section, click Add.

The Add Source page that appears is organized in three sections.

5. In the General Settings section of the Add Source page:

   a. Enter the appropriate value for the following required parameters:

      Name

      A descriptive name of your choice for the connector source.

      Example: My Aha! Content

      Source Type

      The connector used by this source. In this case, select Aha!

      Addresses

      The URL to access your Aha! content, typically in the form:

      https://[domain].aha.io/

      where you replace [domain] by your Aha! domain.
Fields

If you created an Aha! field set, select it.

Refresh Schedule

Time interval at which the index is automatically refreshed to keep the index content up-to-date. By default, the Every day option instructs CES to refresh the source everyday at 12 AM.

Because the Aha! connector does not support incremental refresh, keep this value. Consider using a shorter interval when your Aha! content changes frequently within a day and you need to have a better search result freshness.

Note: You can create a new or modify an existing source refresh schedule.

b. Review the value for the following parameters that often do not need to be modified:

Rating

Change this value only when you want to globally change the ranking associated with all items in this source relative to the rating of other sources.

Example: If this source is for a legacy PLM, you may want to set this parameter to Low, so that in the search interface, results from this source appear later in the list compared to those from other sources.

Document Types

If you created a custom document type set for this source, select it. Otherwise, leave Default.

Active Languages

If you defined custom active language sets, ensure to select the most appropriate for this source.

6. In the Specific Connector Parameters & Options section of the Add Source page:

   a. In the Access token box, paste the access_token value that you obtained previously (see "Granting the Connector Access to Your Aha! Content" on page 742).

   b. In the Mapping File box, leave the default mapping file name
In the Option section, the state of check boxes generally does not need to be changed:

Index Subfolders

Check to index all subfolders below the specified starting addresses.

Index the document’s metadata

When selected, CES indexes all the document metadata, even metadata that are not associated with a field. The orphan metadata are added to the body of the document so that they can be searched using free text queries.

When cleared (default), only the values of system and custom fields that have the Free Text Queries attribute selected will be searchable without using a field query.

**Example:** A document has two metadata:

- LastEditedBy containing the value Hector Smith
- Department containing the value RH

In CES, the custom field CorpDepartment is bound to the metadata Department and its Free Text Queries attribute is selected.

When the Index the document’s metadata option is cleared, searching for RH returns the document because a field is indexing this value. Searching for hector does not return the document because no field is indexing this value.

When the Index the document’s metadata option is selected, searching for hector also returns the document because CES indexed orphan metadata.

Generate a cached HTML version of indexed documents

When you select this check box (recommended), at indexing time CES creates HTML versions of indexed documents and saves them in the unified index. In the search interfaces, users can then more rapidly review the content by clicking the Quick View link to open the HTML version of the item rather than opening the original document with the original application.

Consider clearing this check box only if you do not want to use Quick View links or to save resources when building the source.

Open results with cached version

Leave this check box cleared (recommended) so that in the search interfaces, the main search result link opens the original document with the original application. Consider selecting this check box only when you do not want users to be able to open the original document but only see the HTML version of the document as a Quick View. When this option is selected, you must also select the Generate a cached HTML version of indexed documents check box.

d. Click Save to save the source configuration.

7. In the Security section of the Add Source page:
a. In the **Security Provider** drop-down list, select a security provider such as **Email** that resolves permissions to emails (like the Aha! connector does) so that users authenticated with their email address in a Coveo search interface can see the Aha! content to which they have the read permission.

b. Click **Save and Start** to save your source configuration and start indexing.

### 9.3 Alfresco One Connector

**CES 7.0.8225+ (March 2016)**

Alfresco One is an Enterprise Content Management (ECM) platform designed to store, share, and manage organization documents.

This Coveo connector for Alfresco One allows Coveo administrators to crawl and index the Alfresco content repository. The indexed content is then integrated into the Coveo unified index. The connector indexes all files and the attached permissions so that in the Coveo search interfaces, a user can easily find any but only content to which he has access in Alfresco One.

**Note:** The connector also supports Alfresco Community Edition, but not Alfresco Cloud Edition.

The features of the Alfresco One connector are:

**Content Indexing**

The connector can retrieve and index exclusively the following default Alfresco One content repository entity types:

- Documents
- Records
- AlfrescoFolders
  - Spaces
  - Sites
  - Folders
  - Categories

**Note:** Currently, only comments and likes on discussion forum topics are indexed, meaning that site, document library, document, and blog post comments and likes are ignored during the crawling process.
Fully Supported Security Model

The connector fully supports the Alfresco One security model. This means that, in the Coveo search interface, a user searching Alfresco One content only sees the content to which he has access in Alfresco One.

Incremental Refresh

Periodically queries the Alfresco One system for the latest items modifications (addition, edition, deletion), keeping the index content up-to-date.

Notes:

- Auditing must be enabled for indexed entities for the connector to be able to retrieve items modification (see Enabling Auditing in Alfresco).
- When auditing is not enabled, incremental refreshes are performed as full refreshes.

What's Next?

Review the deployment process (see "Alfresco One Connector Deployment Overview" on page 749).

9.3.1 Alfresco One Connector Deployment Overview

The following procedure outlines the steps needed to deploy the Alfresco One connector. The steps indicate the order in which you must perform configuration tasks on both the CES and Alfresco One systems.

1. Validate that your environment meets the requirements (see "Alfresco One Connector Requirements" on page 750).

2. In the Alfresco One system:

   a. Select or create the crawling account.

      The connector needs an Alfresco One account with which it can crawl all the Alfresco One content that you want to index (see "Selecting an Alfresco One Full Read Account" on page 751).

   b. Enable auditing of content

      Note: When auditing is not enabled, incremental refreshes are performed as full refreshes.

      i. With a text editor, open the Alfresco One global properties file located in the Alfresco One folder.

      Example: C:\Program Files\Alfresco\tomcat\shared\classes\alfresco-global.properties

      ii. Add one of the following property:

          - audit.enabled=true

          to enable audit in general.
• audit.cmischangelog.enabled=true

to implement the change log feature on your CMIS server.

**Note:** The logs contain all create, read, update, and delete operations that users performed on objects in the Alfresco One repository.

iii. Save the file.
iv. Restart the Alfresco Enterprise service to apply changes.

3. On the Coveo server, in the Coveo Administration Tool:
   a. Configure the user identity
      
      You must assign the selected Alfresco One full-read account to a Coveo user identity.
   
b. Optionally create an Email security provider
      
      When an email is defined for each of your users in Alfresco and this email is used to authenticate them in your Coveo search interface, you can create an Email security provider to allow you to map your Alfresco users to their email (see "Configuring an Email Security Provider" on page 65).
   
c. Create a security provider.
      
      When you want to index permissions, you must configure a security provider (see "Configuring an Alfresco One Security Provider" on page 751).
   
d. Create an Alfresco One field set.
      
      It is recommended to import the out-of-the-box Alfresco One field set ([CES\Path]\Bin\Coveo.CES.CustomCrawlers.Alfresco2.FieldSet.xml to be able to easily add Alfresco One specific facets to your Coveo search interfaces.
   
e. Configure and index the Alfresco One source
      
      The connector needs to know details about the Alfresco One system to be able to index its content (see "Configuring and Indexing an Alfresco One Source" on page 753).
   
f. Optionally, modify hidden source parameters
      
      Once your Alfresco One source is up and running, if you encounter timeout or performance issues, consider modifying some hidden source parameters to try resolving the issues (see "Modifying Hidden Alfresco One Source Parameters" on page 758).
   
g. Optionally, customize the mapping file to fine-tune indexed content
      
      You can customize the connector mapping file to fine-tune the indexed content or to index other default entities in your Alfresco One system (see "Creating a Custom Alfresco One Mapping File" on page 759).

9.3.2 Alfresco One Connector Requirements

Your environment needs to meet the following requirements to be able to use the Coveo connector for Alfresco One systems:
• **CES 7.0.8225+ (March 2016)**
  The connector was introduced with the CES 7.0.8225 March 2016 release.

• Coveo license for the Alfresco One connector
  Your Coveo license must include support for the Alfresco One connector to be able to use this connector.

• Alfresco versions
  - Supported versions:
    - Alfresco One 4 to 4.2.5

  **Note:** An Alfresco prototype connector is also available on demand to index the following versions:
  - Alfresco Community 4.2.c and 4.2.d
  - Deprecated support versions: Alfresco Community 3.3, 3.4
  - Contact Coveo Support to ask the connector files.

  Supported Alfresco products:
  - Alfresco Document Management
  - Alfresco Record Management
  - Alfresco Share

What's Next?

Enable auditing on content (see Alfresco One Connector Deployment Overview).

9.3.3 Selecting an Alfresco One Full Read Account

The Coveo connector needs to connect to the Alfresco One system using an account that has access to all the Alfresco One content that you want to index. An account member of the administrator group (ALFRESCO_ADMINISTRATORS) is the simplest choice.

The connector only reads and does not modify Alfresco One content. Consequently, in your Alfresco One system, you can select an existing account or create a new account that has full access to the Alfresco One content that you want to index. A best practice is to create a fixed password account used exclusively by the Coveo connector.

9.3.4 Configuring an Alfresco One Security Provider

The Coveo Alfresco One connector supports the Alfresco One security model. When you want users searching for Alfresco One items in a Coveo search interface to only see the items to which they have access in Alfresco One, the connector needs a security provider to be able to index the permissions for each indexed item.

**Note:** You can get familiar with how Coveo components deal with permissions on documents both at indexing and query time.
To configure an Alfresco One security provider

1. On the Coveo server, access the Administration Tool.
2. Select **Configuration** > **Security**.
3. In the navigation panel on the left, click **Security Providers**.
4. In the **Security Providers** page, click **Add** to create a new security provider.
5. In the **Modify Security Provider** page:

![Security Provider Configuration](image)

a. Configure the following required parameters:

   **Name**
   
   Choose a meaningful name to identify the security provider.
   
   *Example: Alfresco One Security Provider*

   **Security Provider Type**
   
   In the drop-down list, select **Alfresco One (x64)**.
User Identity
Select the Alfresco One user identity that you created previously (see Alfresco One Connector Deployment Overview).

b. Configure the following required parameters:

Alfresco URL
The URL of your Alfresco One content repository server.

Example: https://MyAlfrescoOneServer:[port]/share

Note: You will enter the same value when configuring the source (see “Configuring and Indexing an Alfresco One Source” on page 753).

Alfresco CMIS 1.0 API URL
The URL of the CMIS 1.0 Atom endpoint of the Alfresco One instance. Leave blank to use the default one.

Example: http://MyAlfrescoOneServer:[port]/api/ [RepositoryName]/cmis/versions/1.0/atom

Alfresco REST API URL
The URL of the REST API Endpoint of the Alfresco One Instance. Leave blank to use default one which is your Alfresco One repository server URL followed by alfresco/service/cmis.

Example: https://MyAlfrescoOneServer:[port]/alfresco/service/cmis

Security Provider
Select the security provider that you selected or created to allow this security provider to resolve and expand the groups (see Alfresco One Connector Deployment Overview).

Note: The Alfresco security provider can be chained with either an Active Directory or an Email security provider.

c. Leave the Allow Complex Identities cleared as it does not apply to this type of security provider.

d. Click Apply Changes.

What’s Next?
Create and index a source (see "Configuring and Indexing an Alfresco One Source" on page 753).

9.3.5 Configuring and Indexing an Alfresco One Source
A source defines a set of configuration parameters for a specific Alfresco One system.
To configure and index an Alfresco One source

1. On the Coveo server, access the Administration Tool.
2. Select Index > Sources and Collections.
3. In the Collections section:
   a. Select an existing collection in which you want to add the new source.
   OR
   b. Click Add to create a new collection.
4. In the Sources section, click Add.
5. In the General Settings section of the Add Source page:

   a. Enter the appropriate value for the following required parameters:

      Name
      Enter a descriptive name of your choice for the connector source.
      
      Example: Corporate Alfresco One Server

      Source Type
      Select the connector used by this source. In this case, select Alfresco One.
Note: If you do not see Alfresco One in the Source Type list, ensure that your environment meets the requirements (see "Alfresco One Connector Requirements" on page 750).

Addresses

The URL to the Alfresco One content repository server in the following format:

The root address of the Alfresco organization in the format:

http://[serverName]:[port]/share

where you replace [serverName]:[port] by the host name and port of your Alfresco One server.

Note: When you want to index more than one Alfresco One server or more than one organization, the best practice is to enter only one address here for one server/organization, and then create other sources for other servers or organizations.

b. The following parameters generally do not need to be changed:

Rating

Change this value only when you want to globally change the rating associated with all items in this source relative to the rating of items from other sources.

Example: If this source was for a legacy system, you may want to set this parameter to Low, so that in the search interface, results from this source appear later in the list compared to those from other sources.

Document Types

If you defined custom Document Type sets, ensure to select the most appropriate for this source.

Active Languages

If you defined custom Active Language sets, ensure to select the most appropriate for this source.

Fields

Select the field set that you created earlier (see Alfresco One Connector Deployment Overview).

Refresh Schedule

Time interval at which the source is automatically refreshed to keep the index content up-to-date. By default, the Every day option instructs CES to refresh the source everyday at 12 AM. Because the incremental refresh (supported when auditing is enabled) takes care of maintaining the source up-to-date, you can select a longer interval such as Every Sunday.

6. In the Specific Connector Parameters & Options section of the Add Source page:
a. Review the value for the following parameters that often do not need to be modified:

**Number of Refresh Threads**

Determines the number of refresh threads that allow the connector to crawl web pages in parallel. The default value is 2 threads.

**Mapping File**

The path to the mapping file. Leave the default value to use the default mapping file that comes with the connector (Coveo.CES.CustomCrawlers.Alfresco2.MappingFile.xml). If you create a custom mapping file, enter the full path to your custom mapping file (see "Creating a Custom Alfresco One Mapping File" on page 759). Contact Coveo Support for assistance if you need to customize the mapping file.

b. In the Parameter section, click Add Parameter when you want to show advanced source parameters (see "Modifying Hidden Alfresco One Source Parameters" on page 758).

c. In the Option section, review the default value of the following check boxes:

**Index Subfolders**

Leave this check box cleared. The connector for this type of source does not use this parameter.

**Index the document’s metadata**

When selected, CES indexes all the document metadata, even metadata that are not associated with a field. The orphan metadata are added to the body of the document so that they can be searched using free text queries.

When cleared (default), only the values of system and custom fields that have the Free Text Queries attribute selected will be searchable without using a field query.
Example: A document has two metadata:

- LastEditedBy containing the value Hector Smith
- Department containing the value RH

In CES, the custom field CorpDepartment is bound to the metadata Department and its Free Text Queries attribute is selected.

When the Index the document’s metadata option is cleared, searching for RH returns the document because a field is indexing this value. Searching for hector does not return the document because no field is indexing this value.

When the Index the document’s metadata option is selected, searching for hector also returns the document because CES indexed orphan metadata.

Document’s addresses are case-sensitive

Leave this check box cleared. This parameter needs to be checked only in rare cases for systems in which distinct documents may have the same name but different casing (for example: mydocument and MyDocument).

Generate a cached HTML version of indexed documents

When you select this check box (recommended), at indexing time, CES creates HTML versions of indexed documents. In the search interfaces, users can then more rapidly review the content by clicking the Quick View link rather than opening the original document with the original application.

Consider clearing this check box only if you do not want to use Quick View links or to save resources when building the source.

Open results with cached version

Leave this check box cleared (recommended) so that in the search interfaces, the main search result link opens the original document with the original application.

Consider selecting this check box only when you do not want users to be able to open the original document but only see the HTML version of the document as a Quick View. In this case, you must also select Generate a cached HTML version of indexed documents.

7. In the Security section of the Add Source page:
a. In the **Security Provider** drop-down list, when you chose to use a security provider, select the security provider that you created for this source (see "Configuring an Alfresco One Security Provider" on page 751).

b. In the **Authentication** drop-down list, select the user identity that you created previously for the Alfresco One system (see "Selecting an Alfresco One Full Read Account" on page 751).

8. Click **Save and Start** to save the source configuration and start indexing this source.

9. Validate that the source building process is executed without errors:
   - In the navigation panel on the left, click **Status**, and then validate that the indexing proceeds without errors.

   **OR**

   - Open the CES Console to monitor the source building activities.

9.3.5.1 Modifying Hidden Alfresco One Source Parameters

The **Add Source** and **Source: ... General** pages of the Administration Tool present the parameters with which you can configure the connector for most setups. More advanced and more rarely used parameters are hidden. You can choose to make one or more of these parameters appear in the **Add Source** and **Source: ... General** pages of the Administration Tool so that you can change their default value. Consider changing values of hidden parameters only when you encounter timeout error messages or performance issues.

There is only one advanced hidden parameter for Alfresco One sources. The parameter type (integer, string,...) appears between parentheses following the parameter name.

**NumberOfRetries (Integer)**

The number of retries allowed when a failed web request is recoverable. The default value is 3.

**Timeout (Integer)**

The number of seconds to wait before the request times out (i.e., the time for the server to respond to a request). The default value is 100 seconds.

**ReadTimeout (Integer)**

The timeout in seconds when reading the content from the server. The default value is 300 seconds.

**RepositoryName (Integer)**

The name of the repository to index. The default value is `default`.

**BatchSize (Integer)**

Number of items to fetch per request made to the Alfresco One server. The default value is 25. The minimum value is 1. A small value forces the connector to make small but frequent queries to the Alfresco One server. A larger value leads to larger and less frequent queries.

**CacheTTLInMinutes (Integer)**

The number of minutes an unused cached item (user or CMIS object) can remain in the cache. The default
value is 5 minutes.

Use the following procedure only when you want to modify the above hidden source parameters.

To modify hidden Alfresco One source parameters

1. Refer to "Adding an Explicit Connector Parameter" on page 450 to add an Alfresco One hidden source parameter.

2. For a new Alfresco One source, access the Add Source page of the Administration Tool to modify the value of the newly added advanced parameter:
   a. Select Index > Sources and Collections.
   b. Under Collections, select the collection in which you want to add the source.
   c. Under Sources, click Add.
   d. In the Add Source page, edit the newly added advanced parameter value.

3. For an existing Alfresco One source, access the Source: ... General page of the Administration Tool to modify the value of the newly added advanced parameter:
   a. Select Index > Sources and Collections.
   b. Under Collections, select the collection containing the source you want to modify.
   c. Under Sources, click the existing Alfresco One source in which you want to modify the newly added advanced parameter.
   d. In the Source: ... General page, edit the newly added advanced parameter value, and then click Apply Changes.

9.3.6 Creating a Custom Alfresco One Mapping File

The Alfresco One mapping file exactly determines which types of Alfresco One documents are indexed and where this information is added to the Coveo unified index.

The default mapping file is embedded within the connector and is automatically used when no mapping file is specified in the source.

The default mapping file allows to index the following Alfresco document types:

- Documents
- Records
- AlfrescoFolders
  - Spaces
  - Sites
  - Folders
  - Categories
To create a custom Alfresco One mapping file

1. Using a text editor, create an XML file that respects the Alfresco One mapping file format (see the "Mapping File Format" on page 760 section).

2. Save the file on the Coveo server (recommended folder and filename: [Index_Path] VConfig\Coveo.CES.CustomCrawlers.Alfrescov2.config where by default [Index_Path] = C:\CES7).

3. Specify the mapping file path and filename in the Alfresco One source (see "Configuring and Indexing an Alfresco One Source" on page 753).

Mapping File Format

The mapping file is an XML file that contains various sections and subsections. The root node is <Mappings>. It contains various <CommonMapping> nodes, each defining one type to be indexed.

The first <DefaultMapping> node contains mappings that apply to all entities defined in the mapping file.

The following example contains mappings that add a descriptive title for data lists, todo lists and link items:

```
<Mappings>
  <Version>1</Version>
  <CommonMapping />
  </CommonMapping>
  <Mapping type="F:dl:dataList">
    <Title>%[cmis:description]</Title>
  </Mapping>
  <Mapping type="D:lnk:link">
    <Title>%[lnk:description]</Title>
  </Mapping>
  <Mapping type="D:dl:todoList">
    <Title>%[dl:todoTitle]</Title>
  </Mapping>
  <Mapping type="D:dl:contact">
    <Title>%[dl:contactFirstName] %[dl:contactLastName]</Title>
  </Mapping>
  </DefaultMapping>
</Mappings>
```

9.4 Amazon S3 Connector

**CES 7.0.7711+ (June 2015)**

Amazon simple storage service (S3) is a cloud based object storage, designed to store, distribute and manage a large quantity of data worldwide.

The Coveo connector for Amazon S3 allows Coveo administrators to index and integrate the Amazon S3 content into the Coveo unified index and make it easily searchable by end-users.

**Note:** An access key is needed to connect to the Amazon Web Services (AWS) service through the software development kit (SDK). The access key is a way to authenticate from the SDK as an Identity and Access Management (IAM) account. The number of requests is unlimited, but every request to your Amazon S3 bucket(s) has a charge (see Request Pricing).
9.4.1 Connector Features Summary

<table>
<thead>
<tr>
<th>Features</th>
<th>Supported</th>
<th>Additional information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Amazon S3 version</td>
<td>Latest cloud version</td>
<td>Following available Amazon S3 releases</td>
</tr>
<tr>
<td>Searchable content types †</td>
<td>✔</td>
<td>Buckets 2 and objects (folders and files)</td>
</tr>
<tr>
<td>Content update</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Incremental refresh</td>
<td>✗</td>
<td></td>
</tr>
<tr>
<td>Full refresh</td>
<td>✔</td>
<td></td>
</tr>
<tr>
<td>Rebuild</td>
<td>✔</td>
<td></td>
</tr>
<tr>
<td>Document-level security</td>
<td>✗</td>
<td>Permissions must be manually defined on the source</td>
</tr>
</tbody>
</table>

1- An access key is needed to connect to the Amazon Web Services (AWS) service through the software development kit (SDK). The access key is a way to authenticate from the SDK as an Identity and Access Management (IAM) account. The number of requests is unlimited, but every request to your Amazon S3 bucket(s) has a charge (see Request Pricing).

2- Amazon S3 Requester Pays buckets are not supported.

9.4.2 Features

The Amazon S3 connector features are:

**Content indexing**

The connector can retrieve and index exclusively the following Amazon S3 types of items:

- Buckets
- Objects (folders and files)

**Note:** The connector supports Amazon S3 server-side encryption on object data.

**Pause/Resume**

When indexing Amazon S3 content, the connector can be paused and resumed.

9.4.3 Limitations

- The Amazon S3 connector does not support the Amazon S3 security model. Thus, permissions must be manually defined on the source (see Permissions).
- The Requester Pays feature in Amazon S3 is not supported (see Requester Pays Buckets).
What's Next?

Review the steps to deploy the Amazon S3 connector (see "Amazon S3 Connector Deployment Overview" on page 762).

9.4.4 Amazon S3 Connector Deployment Overview

The following procedure outlines the steps needed to deploy the Amazon S3 connector. The steps indicate the order in which you must perform configuration tasks on the Coveo server.

To deploy the Amazon S3 connector

1. Validate that your environment meets the requirements (see "Amazon S3 Connector Requirements" on page 762).

2. On the Coveo server, in the Coveo Administration Tool:

   a. Create an Amazon S3 field set to take advantage of the available Amazon S3 metadata.

      i. It is recommended to start by importing the default Amazon S3 field set file ([CES_Path]\Bin\Coveo.CES.CustomCrawlers.AmazonS3.FieldSet.xml) to create fields for all the metadata available by default from Amazon S3 documents.

      ii. When you created custom metadata for your Amazon S3 documents, add corresponding fields to the field set.

   b. Configure and index an Amazon S3 source.

      The connector must know details about the authorized access to the Amazon S3 bucket(s) to index its content (see "Configuring and Indexing an Amazon S3 Source" on page 762).

   c. If you encounter issues, verify if modifying the default value of hidden source parameters can help resolve the problems (see "Modifying Hidden Amazon S3 Source Parameters" on page 768).

9.4.5 Amazon S3 Connector Requirements

Your environment must meet the following requirements to be able to use the Amazon S3 connector:

- **CES 7.0.7711+ (June 2015)**

- Coveo license for the Amazon S3 connector

   Your Coveo license must include support for the Amazon S3 connector to be able to use this connector.

- A valid IAM Account

   You need an IAM account with at least the Read permission on the bucket to be crawled.

What's Next?

Create an Amazon S3 field set (see Amazon S3 Connector Deployment Overview).

9.4.6 Configuring and Indexing an Amazon S3 Source

A source defines a set of configuration parameters for indexing the content of a specific Amazon S3 site.
To configure and index an Amazon S3 source

1. On the Coveo server, access the Administration Tool.

2. Select Index > Sources and Collections.

3. In the Collections section:
   a. Select an existing collection in which you want to add the new source.

   OR

   b. Click Add to create a new collection.

4. In the Sources section, click Add.

   The Add Source page that appears is organized in three sections.

5. In the General Settings section of the Add Source page:

   a. Enter the appropriate value for the following required parameters:

      Name

      A descriptive name of your choice for the connector source.

      **Example:** Amazon S3 Site
Source Type

The connector used by this source. In this case, select **Amazon S3**.

Addresses

The address of the Amazon S3 bucket site in one of the following types:

- **Virtual-host style**

  **Examples:**
  - http://[bucket].s3.amazonaws.com/
  - http://[bucket].s3-[aws-region].amazonaws.com/

  where you replace [bucket] by your actual bucket name and [aws-region] with your region-specific endpoint.

- **Path style**

  **Examples:**
  - http://s3.amazonaws.com/[bucket]
  - http://s3-[aws-region].amazonaws.com/[bucket]

  where you replace [bucket] by your actual bucket name and [aws-region] with your region-specific endpoint.

You can enter more than one bucket address on separate lines, but you must ensure that all source parameters apply to all Amazon S3 buckets. Otherwise, create other sources for other buckets.

Notes:

- The starting address must specify one bucket with its region. URLs that do not specify any region are using the US Standard (us-east-1) region endpoint.
- When the URL point to a folder inside a bucket, only keys starting with that prefix will be crawled.
- You can index more than one bucket.

Fields

If you defined an Amazon S3 field set, select it (see Amazon S3 Connector Deployment Overview).

Refresh Schedule

Time interval at which the index is automatically refreshed to keep the index content up-to-date. By default, the Every day option instructs CES to refresh the source everyday at 12 AM.

**Note:** You can create a new or modify an existing source refresh schedule.

b. Review the value for the following parameters that often do not need to be modified:
Rating

Change this value only when you want to globally change the ranking associated with all items in this source relative to the rating of other sources.

**Example:** If this source is for a legacy PLM, you may want to set this parameter to **Low**, so that in the search interface, results from this source appear later in the list compared to those from other sources.

Document Types

If you created a custom document type set for this source, select it. Otherwise, leave **Default**.

Active Languages

If you defined custom active language sets, ensure to select the most appropriate for this source.

6. In the **Specific Connector Parameters & Options** section of the **Add Source** page:

![Specific Connector Parameters & Options]

a. When the Amazon S3 content is private, enter the appropriate value for the following parameters. Otherwise (for public data set) leave them empty:

**Notes:**

- The Access Key and Secret Key are accessible in the IAM console (see [Understanding and Getting Your Security Credentials](#)).
- **CES 7.0.7914+ (October 2015)** The Access Key and Secret Key parameters are optional.

**Access Key**

The ID of the IAM account access key used to request data from the Amazon S3 servers.

**Example:** AKIAIOSFODNN74152KOP
Secret Key

The IAM account secret access key used to request data from the Amazon S3 servers.

Example: wJalrXUtnFEMI/K7MDENG/bPxRfiCYiYc51AYQQf

b. In the Mapping File box, leave the default mapping file name (Coveo.CES.CustomCrawlers.AmazonS3.MappingFile.xml) unless you created a custom mapping file, in which case, enter the full path of your valid mapping file.

c. Click Add Parameter when you want to show and change the value of hidden source parameters (see "Modifying Hidden Amazon S3 Source Parameters" on page 768).

d. In the Option section, the state of check boxes generally does not need to be changed:

Index Subfolders

Check to index all subfolders below the specified starting addresses.

Index the document's metadata

When selected, CES indexes all the document metadata, even metadata that are not associated with a field. The orphan metadata are added to the body of the document so that they can be searched using free text queries.

When cleared (default), only the values of system and custom fields that have the Free Text Queries attribute selected will be searchable without using a field query.

Example: A document has two metadata:

- LastEditedBy containing the value Hector Smith
- Department containing the value RH

In CES, the custom field CorpDepartment is bound to the metadata Department and its Free Text Queries attribute is selected.

When the Index the document's metadata option is cleared, searching for RH returns the document because a field is indexing this value. Searching for hector does not return the document because no field is indexing this value.

When the Index the document's metadata option is selected, searching for hector also returns the document because CES indexed orphan metadata.

Generate a cached HTML version of indexed documents

When you select this check box (recommended), at indexing time CES creates HTML versions of indexed documents and saves them in the unified index. In the search interfaces, users can then more rapidly review the content by clicking the Quick View link to open the HTML version of the item rather than opening the original document with the original application.

Consider clearing this check box only if you do not want to use Quick View links or to save resources when building the source.
Open results with cached version

Leave this check box cleared (recommended) so that in the search interfaces, the main search result link opens the original document with the original application. Consider selecting this check box only when you do not want users to be able to open the original document but only see the HTML version of the document as a Quick View. When this option is selected, you must also select the Generate a cached HTML version of indexed documents check box.

e. Click Save to save the source configuration.

7. Because Amazon S3 security model is not yet supported, the Amazon S3 connector does not index permissions and you must change the default Permissions option to set the permissions globally on the source:

Note: You get the following error message in the CES Console when the Index security permissions option is selected by default:

Permissions indexing is not provided by AmazonS3Crawler.

a. In the navigation panel on the left, select Permissions.

b. In the Permissions page:
i. Select the **Specifies the security permissions to index** option.

ii. In the **Allowed Users** list, add or remove users or groups to precisely specify who has access to the content from this source.

   By default, the Active Directory **everyone** group specifies that any Active Directory user can see all the content from this source.

iii. Optionally, in the **Denied Users** list, add users or groups to specify who has not access to the content from this source.

iv. Click **Apply Changes**.

8. On the toolbar, click **Start/Rebuild** to start indexing your source.

9. Validate that the source building process is executed without errors:
   
   - In the navigation panel on the left, click **Status**, and then validate that the indexing proceeds without errors.

   OR

   - Open the CES Console to monitor the source building activities.

### 9.4.6.1 Modifying Hidden Amazon S3 Source Parameters

The **Add Source** and **Source: ... General** pages of the Administration Tool present the parameters with which you can configure the connector for most Amazon S3 sites. More advanced and more rarely used parameters are hidden. You can choose to make one or more of these parameters appear in the **Add Source** and **Source: ... General** pages of the Administration Tool so that you can change their default value.

The following list describes the available advanced hidden parameters for Amazon S3 sources. The parameter type (integer, string...) appears between parentheses following the parameter name.

#### BatchSize (Integer)

   The number of objects to retrieve by request (between 1 and 1000). The default value is 100.

To modify hidden Amazon S3 source parameters

1. Refer to "Adding an Explicit Connector Parameter" on page 450 to add one or more Amazon S3 hidden source parameters.

   For a new Amazon S3 source, access the **Add Source** page of the Administration Tool to modify the value of the newly added advanced parameter:

2.

   a. Select **Index > Sources and Collections**.

   b. Under **Collections**, select the collection in which you want to add the source.

   c. Under **Sources**, click **Add**.

   d. In the **Add Source** page, edit the newly added advanced parameter value.
3. For an existing Amazon S3 source, access the Source: ... General page of the Administration Tool to modify the value of the newly added advanced parameter:
   a. Select Index > Sources and Collections.
   b. Under Collections, select the collection containing the source you want to modify.
   c. Under Sources, click the existing Amazon S3 source in which you want to modify the newly added advanced parameter.
   d. In the Source: ... General page, edit the newly added advanced parameter value.

9.5 Atlassian Confluence Legacy Connector

*Deprecated*

The Coveo Legacy connector for Atlassian Confluence allows Coveo administrators to index and integrate the content of Confluence Wiki sites and spaces into the Coveo unified index, making it easily searchable by end-users.

**Important:** The Atlassian Confluence Legacy Connector is now deprecated. To index Atlassian Confluence content, use the second-generation Confluence connector.

### 9.5.1 Connector Features Summary

<table>
<thead>
<tr>
<th>Features</th>
<th>Supported</th>
<th>Additional information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Confluence version</td>
<td>5.5 to 5.8.5 and Cloud</td>
<td></td>
</tr>
<tr>
<td>Searchable content types</td>
<td>✓</td>
<td>Spaces, pages (such as Wiki pages), blog posts, comments on pages and blog posts (included as metadata), and attachments (in pages, blog posts, and comments)</td>
</tr>
<tr>
<td>Content update</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Incremental refresh</td>
<td>✗</td>
<td></td>
</tr>
<tr>
<td>Full refresh</td>
<td>✓</td>
<td>Rebuild needed to apply space name changes (if any) to all space pages.</td>
</tr>
<tr>
<td>Rebuild</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Document-level security</td>
<td>✓</td>
<td>• Requires the Coveo plug-in for on-premises Confluence instances.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Not supported for Confluence Cloud</td>
</tr>
</tbody>
</table>

### 9.5.2 Features

The Confluence connector features are:
• Extraction and indexing of all Confluence item types:
  ○ Spaces
  ○ Wiki pages
  ○ News items (blog posts)
  ○ Comments
  ○ Attachments (binary documents)
• Extraction and indexing of document permissions (supports LDAP integrations, including Active Directory).
• Extraction and indexing of labels.
• Supports the Confluence security model by indexing document permissions (for on-premises deployments when the plugin is installed) so that in Coveo search interfaces, a user searching Confluence content only sees the content to which he has access in Confluence.

Note: The Coveo search interface includes a Quick View of Confluence content and provides Confluence specific facets based on spaces, object types (Page, Comment...), and labels.

9.5.3 Limitations

• The Confluence connector does not support incremental refresh. A source full refresh is required to update the source content.

• If you change the name of a space in Confluence, a full refresh detects the change only for pages created or modified following the change. You must rebuild the source to get the space name change on all space pages.

What’s Next?

Review the steps to deploy the Confluence connector (see "Atlassian Confluence Legacy Connector Deployment Overview" on page 770).

9.5.4 Atlassian Confluence Legacy Connector Deployment Overview

The following procedure outlines the steps needed to deploy the Confluence connector. The steps indicate the order in which you must perform configuration tasks on both the Confluence and Coveo servers.

To deploy the Confluence Legacy connector

1. Validate that your environment meets the requirements (see "Atlassian Confluence Legacy Connector Requirements" on page 772).

2. On your Confluence server:
   a. Enable the Confluence remote API.
      The Confluence connector requires the Confluence SOAP remote API (Web service) to be enabled on your Confluence server (see the Atlassian document Enabling the Remote API).
   b. For an on-premises deployment, optionally install the Coveo plugin.
With Confluence version 3.5.0, 4.x, and 5.8.5 installations, when you want to index permissions, you must install the Coveo Confluence plugin on your Confluence server (see "Installing the Coveo Plugin for Atlassian Confluence" on page 773).

Note:
- Indexing permissions associated with each Confluence object is recommended as it allows the Coveo search interface to only show Confluence documents to which the end-user performing the search has access in Confluence.
- Because you cannot install the Coveo Confluence plugin in Confluence On-Demand, Coveo cannot index permissions for this content.

3. On the Coveo server:
   a. Create a user identity.

      When you want to index permissions, when your Confluence server does not allow anonymous users to access the SOAP remote API, or when you want to crawl using a specific Confluence user, you must create a user identity and set up your Confluence source to use this user identity (see "Adding a User Identity" on page 420).

      With Confluence version 3.5.0, 4.x, and 5.8.5 installations, when you want to index permissions, a user identity is also required and it must refer to a Confluence administrator account.

      Note: When configuring the source, you must use the credentials of a native Confluence user. Users managed by other identity providers such as Google are not supported.

   b. When you want to index permissions, create a security provider.

      For all on-premises supported Confluence versions, when you want to index permissions, you must configure a security provider (see "Creating a Security Provider for the Atlassian Confluence Legacy Connector" on page 777).

   c. Configure and index the Confluence source.

      The Coveo connector needs to know details about your Confluence installation to be able to index its content (see "Configuring and Indexing an Atlassian Confluence Source With the Legacy Connector" on page 780).

4. In the Interface Editor, consider adding Confluence specific items to your Coveo .NET Front-End search interface:
   a. Add the built-in Confluence facets.

      CES comes with three built-in Confluence facets (Space, Type, Label) that you can add to your search interface so that end-users can more easily refine Confluence content in search results (see "Managing Built-in Facets and Related Results Appearing in a .NET Search Interface" on page 574).

   b. Add the Confluence Labels display field.
In the search results, you can make the **Confluence Labels** value appear for each Confluence document using the `syscflabels` field (see "Adding Display Fields to Search Results With the .NET Interface Editor" on page 620).

c. **Integrate a Coveo .NET search interface in Confluence**

You can replace the Confluence search page by a Coveo search interface (see Integrating Coveo .NET Search UI in Confluence). This is particularly useful when your Coveo index contains several other sources, bringing this content into Confluence through the search interface.

d. **Add a Confluence security provider to an outside Confluence search interface**

When a Coveo .NET Front-End search interface used to search for Confluence content is not integrated in Confluence, you must add a security provider to the search interface to allow each user to log in to the search interface with their Confluence credentials, and then be able to see, in the search results, the secured Confluence content for which they have read permissions.

### 9.5.5 Atlassian Confluence Legacy Connector Requirements

Your environment must meet the following requirements to be able to use the Coveo Legacy connector for Confluence:

- **Coveo license for the Confluence Legacy connector**

  Your Coveo license must include support for the Confluence Legacy connector to be able to use this connector.

- **Confluence versions:**

  The connector supports Atlassian Confluence installations using the Confluence SOAP remote API (Web service).

  - **Supported versions:**
    
    - **Cloud**
      
      **Notes:**
      
      - Supported as long as the Confluence SOAP remote API is available for Confluence Cloud.
      - The connector cannot index document level permissions, because the required Coveo plugin cannot be installed in an Atlassian Cloud instance.

      - **5.5 to 5.8.5**

        - Deprecated support versions: 2.5.3, 3.x, 4.x, 5.4

- **Open the Confluence port**

  When the Coveo Master server and the Confluence server are separated by a firewall or another network infrastructure restricting the communication, the Confluence server port (default is 8090) must be opened to allow the Coveo connector to access the content.
What's Next?

Enable the Confluence remote API needed by the Confluence Legacy connector (see the Atlassian document Enabling the Remote API).

9.5.6 Installing the Coveo Plugin for Atlassian Confluence

The Coveo Legacy connector for Confluence comes with a Confluence plugin. The connector needs the plugin to index permissions associated with each Confluence item so that users only see Confluence content to which they have access in Coveo search results. It is therefore recommended to install the plugin for Confluence 3.5.x, 4.x, and 5.8.5 on-premises installations.

Without the plugin, you must set the permissions globally on the source (see Configuring and Indexing an Atlassian Confluence Source With the Legacy Connector), and all indexed Confluence content is searchable by anyone that has the permissions to view the source content.

Notes:

- The Coveo plugin cannot be installed in Confluence Cloud and consequently, permissions associated with each Confluence item cannot be indexed.
- The Coveo plugin is distributed with CES and is not available from the Atlassian Marketplace.
- **CES 7.0.7183+ (November 2014)** The Coveo Plugin for Atlassian Confluence is updated to version 1.01 to allow to specify an email security provider inside the Confluence security provider (see “Creating a Security Provider for the Atlassian Confluence Legacy Connector” on page 777).

To install or update the Coveo Confluence Plugin

1. Log into your Confluence server using a Confluence administrator account.
2. On the menu, click **Browse > Confluence Admin.**
3. If the **Administrator Access** dialog box appears, enter your administrator account credentials, and then click **Confirm**.
4. In the navigation panel on the left, under **Atlassian Marketplace**, click **Manage add-ons**.
5. In the **Manage add-ons** page, click the **Upload add-on** link.
6. In the **Upload add-on** dialog box:
a. Click Choose File.

b. In the Open dialog box, select the [CES_Path]\Bin\Coveo.CES.CustomCrawlers.Confluence.Plugin.jar file from your Coveo Master server, and then click Open.

c. Click Upload.

7. In the Installed and ready to go! dialog box, click Close.
Note: CES 7.0.8225–(March 2016) In the Confluence Manage add-ons page, the Coveo plugin reports being v. 1 even if it is actually version 1.0.1.

Installed and ready to go!

Coveo Enhanced Soap API Plugin  v. 1
by Coveo

This add-on has been installed. If you need help getting started, click the link to the add-on documentation from the Manage add-ons screen.

You can see the actual plugin version in the CES index logs by looking for the message in the form:

Confluence plugin version is: [pluginVersion]

8. In the User-installed add-ons list, validate that the Coveo Enhanced Soap API Plugin is listed.
Note: If you reinstall or upgrade the Coveo plugin on your Confluence instance, you must restart the Confluence service to overcome a known Confluence issue that causes Confluence to return an `IllegalArgumentException` when the Coveo plugin is used, preventing to index your Confluence source (see Broken Webservice when redeploying RPC Plugin Module).

When this issue occurs, you can get error messages similar to the followings depending on your CES version:

- **CES 7.0.8388+ (June 2016)** `CONFLUENCE_LEGACY_PLUGIN_UNABLE_TO_CONNECT`
- **CES 7.0.8225– (March 2016)**

```java
```

To uninstall the Coveo Confluence plugin

1. Log into your Confluence server using a Confluence administrator account.
2. On the menu, click Browse > Confluence Admin.
3. If the Administrator Access dialog box appears, enter your administrator account credentials, and then click Confirm.
4. In the navigation panel on the left, under Atlassian Marketplace, click Manage add-ons.
5. In the User-installed add-ons list, locate and expand Coveo Enhanced Soap API Plugin.
6. In the Coveo Enhanced Soap API Plugin section, click Uninstall.
7. In the Confirm dialog box, click Continue.

8. Validate the Coveo Enhanced Soap API Plugin is no longer listed in the User-installed add-ons list.

9.5.7 Creating a Security Provider for the Atlassian Confluence Legacy Connector

For an on-premises Confluence, when you choose to index document permissions associated with Confluence items, the Coveo connector needs a security provider. When document permissions are indexed, in Coveo search results, a user searching for Confluence content only sees the content to which he has access in Confluence.

Note: You can get familiar with how Coveo components deal with permissions on documents both at indexing and query time.

To configure a Confluence security provider

1. On the Coveo server, access the Administration Tool.


3. In the navigation panel on the left, click Security Providers.

4. In the Security Providers page, click Add to create a new security provider.

5. In the Modify Security Provider page:
a. Configure the following required parameters:

**Name**

Choose a significant name to identify the security provider.

**Example**: Confluence Security Provider

**Security Provider Type**

Select Confluence (x64).

**User Identity**

Select the Confluence user identity that you created previously (see "Adding a User Identity" on page [4](#) of the Administrator Guide.)
Security Provider

Select **Active Directory** or a custom Active Directory security provider that you created for a specific domain to allow this Confluence security provider to map Confluence permissions to AD users.

**CES 7.0.7183+ (November 2014)** You can select an email security provider to allow this Confluence security provider to map Confluence permissions to emails. This is useful when your users are authenticated in the search interface with the same email address specified for their Confluence user, thus allowing them to also see secured documents to which they have read permissions.

**Note:** Connecting to an email security provider requires the plugin version 1.0.1+ (see "Installing the Coveo Plugin for Atlassian Confluence" on page 773).

Web Service URL

The address of the Confluence server. This should be the same address as the one that you will specify when you configure the source for the connector (see "Configuring and Indexing an Atlassian Confluence Source With the Legacy Connector" on page 780). Enter the URL in the following format:

http://[ConfluenceServer]:[port]

**Example:** http://MyConfluenceServer:8090

Enhanced Web Service URL

For Confluence version 3.5.0 to 5.8.5 installations, you must enter the URL pointing to the Coveo web service provided by the Coveo plugin on the Confluence server in the following format:

http://[ConfluenceServer]:[port]/rpc/soap-axis/coveo-enhanced-service

**Example:** http://MyConfluenceServer:8090/rpc/soap-axis/coveo-enhanced-service

Authenticate Connection

Select this check box when you selected your Confluence user identity in **User Identity** to use it to authenticate the connection when connecting to the Confluence web services. The check box is cleared by default.

b. For a Confluence 2.5.3 to 3.4.x installation, include the following required parameters:

**DB Connection String**

A valid database connection string to allow the connector to retrieve the security information from the Confluence database.

**Example:**
server=MyServer;database=MyDatabase;
User=MyUser;Password=MyPassword

**Database Driver Type**

Driver type to use to connect to the Confluence database. Possible values are: SqlClient, OleDb, or Odbc.
LDAP Configuration File

For LDAP integrations only, path of the Confluence LDAP configuration file (atlassian-user.xml) from which the connector automatically extracts the LDAP connection settings.

Example: \\server\c$\confluence\WEB-INF\classes\atlassian-user.xml

**Note:** When your Confluence server has an LDAP integration, the Confluence connector must also connect to the LDAP servers to extract the information of the LDAP members and to retrieve the members of LDAP groups (see the Atlassian document Connecting to an LDAP Directory).

User Management Framework

Default Confluence user management framework to use (see the Atlassian document Understanding User Management in Confluence). Possible values are: Default, AtlassianUser, or OSUser. This parameter is optional.

**c.** Consider revising the default value of the following parameters:

**Time to Live**

Number of milliseconds before refreshing the cache of members. The default value is 300000 ms (5 minutes).

**Web Service Connection Timeout**

Maximum number of milliseconds a Web service call should wait. The default value is 300000 ms (5 minutes).

**Allow Complex Identities**

Leave this option cleared as it does not apply to this type of security provider.

**d.** Click Apply Changes.

What's Next?

Configure and index a Confluence source (see "Configuring and Indexing an Atlassian Confluence Source With the Legacy Connector" on page 780).

9.5.8 Configuring and Indexing an Atlassian Confluence Source With the Legacy Connector

A source defines a set of configuration parameters for a specific Confluence site.

To configure and index a Confluence source

1. On the Coveo server, access the Administration Tool.
2. Select Index > Sources and Collections.
3. In the Collections section:
   a. Select an existing collection in which you want to add the new source.

   OR
b. Click **Add** to create a new collection.

4. In the **Sources** section, click **Add**.

   The **Add Source** page that appears is organized in three sections.

5. In the **General Settings** section of the **Add Source** page:

   ![Add Source page](image)

   a. Enter the appropriate value for the following required parameters:

   **Name**

   A descriptive name of your choice for the connector source.

   **Example:** Corporate Confluence Wiki

   **Source Type**

   The connector used by this source. In this case, select **Confluence**.

   **Note:** If you do not see **Confluence** in the **Source Type** list, ensure that your environment meets the requirements (see "Atlassian Confluence Legacy Connector Requirements" on page 772).

   **Addresses**

   List of starting points for the connector, one address per line.
Examples: Use the Confluence server root URL as the starting address to index a complete Confluence site:

http://MyConfluenceServer:8090/

To index specific spaces, add their URL as starting addresses:

http://MyConfluenceServer:8090/display/space1
http://MyConfluenceServer:8090/display/space2

where space1 and space2 the Confluence spacekey for the desired space.

To index Confluence Cloud content:

https://MyCompany.atlassian.net/wiki/

Notes:

- To be able to index document permissions, all your starting points must be located on a single Confluence site. Create separate sources for separate sites.

- CES 7.0.6830+ (July 2014) You can enter specific space addresses for deployments where Confluence is not installed at the server root such as:

  http://server/MyConfluence/display/space1name.

b. The following parameters often do not need to be changed:

Rating

Change this value only when you want to globally change the rating associated with all items in this source relative to the rating of other sources.

Example: When the source indexes a legacy repository, you may want to set this parameter to Low, so that in the search interface, results from this source appear lower in the list compared to those from active repository sources.

Document Types

If you defined a custom document type set for this source, select it.

Active Languages

If you defined custom active language sets, ensure to select the most appropriate for this source.

Fields

If you defined custom field sets, ensure to select the most appropriate for this source.

Refresh Schedule

Time interval at which the index is automatically refreshed to keep the index content up-to-date. By default, the Every day option instructs CES to refresh the source everyday at 12 AM.

6. In the Specific Connector Parameters & Options section of the Add Source page:
a. Next to **Parameters**, for Confluence version 2.x to 3.4.x installations, when you chose to index permissions, click **Add Parameter** to add the **DBConnectionString**, **DBDriverType**, and **LDAPConfigFilePath** mandatory source parameters with the same value entered for the security provider (see "Creating a Security Provider for the Atlassian Confluence Legacy Connector" on page 777).

![Parameters Table]

**Note:** Other advanced parameters are also available (see "Modifying Hidden Atlassian Confluence Source Parameters for the Legacy Connector" on page 786).

b. The **Option** check boxes generally do not need to be changed:

**Index Subfolders**

Keep this check box selected (recommended). By doing so, all subfolders from the specified server address are indexed.

**Index the document's metadata**

When selected, CES indexes all the document metadata, even metadata that are not associated with a field. The orphan metadata are added to the body of the document so that they can be searched using free text queries.

When cleared (default), only the values of system and custom fields that have the **Free Text Queries** attribute selected will be searchable without using a field query.
Example: A document has two metadata:
- LastEditedBy containing the value Hector Smith
- Department containing the value RH

In CES, the custom field CorpDepartment is bound to the metadata Department and its Free Text Queries attribute is selected.

When the Index the document’s metadata option is cleared, searching for RH returns the document because a field is indexing this value. Searching for hector does not return the document because no field is indexing this value.

When the Index the document’s metadata option is selected, searching for hector also returns the document because CES indexed orphan metadata.

Document’s addresses are case-sensitive

Leave the check box cleared. This parameter needs to be checked only in rare cases for systems in which distinct documents may have the same name but different casing.

Generate a cached HTML version of indexed documents

When you select this check box (recommended), at indexing time, CES creates HTML versions of indexed documents. In the search interfaces, users can then more rapidly review the content by clicking the Quick View link rather than opening the original document with the original application. Consider clearing this check box only when you do not want to use Quick View links or to save resources when building the source.

Open results with cached version

Leave this check box cleared (recommended) so that in the search interfaces, the main search result link opens the original document with the original application. Consider selecting this check box only when you do not want users to be able to open the original document but only see the HTML version of the document as a Quick View. In this case, you must also select Generate a cached HTML version of indexed documents.

7. In the Security section of the Add Source page:
a. In the **Security Provider** drop-down list, if you chose to index permissions, select the Confluence security provider that you created for this source (see "Creating a Security Provider for the Atlassian Confluence Legacy Connector" on page 777), otherwise, select **None**.

b. In the **Authentication** drop-down list, if you chose to index permissions, select the Confluence crawling user identity that you created for this source. Otherwise, select **None**.

c. Click **Save** to save the source configuration.

8. When you chose to NOT index permissions, you must set the permissions globally for the source:

   a. In the navigation menu on the left, select **Permissions**.

   b. Next to **Permissions**, select the **Specifies the security permissions to index** option.

   c. Next to **Allowed Users**, ensure that a well-known everyone group such as the Active Directory $S-1-1-0$ is added.

   d. Click **Apply Changes**.
Note: You may need to enable the anonymous access to the remote API for your Confluence site (see Anonymous Access to Remote API) to prevent getting an error message similar to the following one in the CES Console or logs:

```
Cannot load the provided starting address: http://ConfluenceServer:8090/ --> Unable to connect to this address: 'http://ConfluenceServer:8090/' --> SoapException --> com.atlassian.confluence.rpc.NotPermittedException: Anonymous RPC access is disabled on this server
```

9. Validate that the source building process is executed without errors:

- In the navigation panel on the left, click **Status**, and then validate that the indexing proceeds without errors.

  OR

- Open the CES Console to monitor the source building activities.

What's Next?

Add the built-in the Confluence facet to your search interface (see "Managing Built-in Facets and Related Results Appearing in a .NET Search Interface" on page 574).

9.5.9 Modifying Hidden Atlassian Confluence Source Parameters for the Legacy Connector

The **Add Source** and **Source: ... General** pages of the Administration Tool present the parameters with which you can configure the connector for most Confluence setups. More advanced and more rarely used parameters are hidden. You can choose to make one or more of these parameters appear in the **Add Source** and **Source: ... General** pages of the Administration Tool so that you can change their default value. Consider changing values of hidden parameters when you encounter issues.

The following list describes the advanced hidden parameters available with Confluence sources. The parameter type (integer, string,...) appears between parentheses following the parameter name.

**WebServiceConnectionRetryCount (Integer)**

Maximum number of retries to perform when a Web service call fails. The default value is 3.

**WebServiceConnectionRetryDelay (Integer)**

Number of milliseconds to wait before retrying when a Web service call fails. The default value is 30000 ms (30 seconds).

**WebServiceConnectionTimeout (Integer)**

Maximum number of milliseconds a Web service call should wait. The default value is 30000 ms (30 seconds).

**EnhancedWebServiceUrl (String)**

For Confluence version 3.5.0, 4.x, and 5.8.5 the enhanced web service URL pointing to the Coveo web service provided by the Coveo plugin installed on the Confluence server.

Example: `http://MyConfluenceServer:8090/rpc/soap-axis/coveo-enhanced-service`
For Confluence version 2.5.3 to 3.4.x installations only

**DBConnectionString (String)**
- Required parameter describing the string used by the source to connect to the Confluence database.

**DBDriverType (String)**
- Required parameter specifying the driver type to use to connect to the Confluence database. Possible values are: SqlClient, OleDb, or Odbc.

**LDAPConfigFilePath (String)**
- When your Confluence site uses LDAP integration, required parameter specifying the path of the Confluence LDAP configuration file (atlassian-user.xml).

**Example:** `\server\c$\confluence\WEB-INF\classes\atlassian-user.xml`

**UserManagementFramework**
- Optional parameter specifying the default Confluence user management framework to use (see the Atlassian document Understanding User Management in Confluence). Possible values are: Default, AtlassianUser, or OSUser.

Use the following procedure only when you want to modify one or more of the above hidden source parameters.

To modify hidden Confluence source parameters

1. Refer to "Adding an Explicit Connector Parameter" on page 450 to add one or more Confluence hidden source parameters.

2. For a new Confluence source, access the Add Source page of the Administration Tool to modify the value of the newly added advanced parameter:
   a. Select Index > Sources and Collections.
   b. Under Collections, select the collection in which you want to add the source.
   c. Under Sources, click Add.
   d. In the Add Source page, edit the newly added advanced parameter value.

3. For an existing Confluence source, access the Source: ... General page of the Administration Tool to modify the value of the newly added advanced parameter:
   a. Select Index > Sources and Collections.
   b. Under Collections, select the collection containing the source you want to modify.
   c. Under Sources, click the existing Confluence source in which you want to modify the newly added advanced parameter.
   d. In the Source: ... General page, edit the newly added advanced parameter value.

4. Rebuild your Confluence source to apply the changes to the parameters.
9.6 Atlassian Confluence V2 Connector

CES 7.0.8225+ (March 2016)

The second-generation (V2) Coveo connector for Atlassian Confluence allows Coveo administrators to index and integrate the content of Confluence Wiki sites and spaces into the Coveo unified index, making it easily searchable by end-users.

9.6.1 Connector Features Summary

<table>
<thead>
<tr>
<th>Features</th>
<th>Supported</th>
<th>Additional information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Confluence version</td>
<td>6.7 to 7.1 and Cloud</td>
<td></td>
</tr>
<tr>
<td>Searchable content types</td>
<td></td>
<td>Spaces, pages (such as Wiki pages), blog posts, comments on pages and blog posts (included as metadata), and attachments (in pages, blog posts, and comments)</td>
</tr>
<tr>
<td>Content update</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Incremental refresh</td>
<td></td>
<td>(Confluence only) Requires the Coveo plugin to retrieve deleted, restored, and moved items, and items with modified comments or permissions.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>(Confluence Cloud only) Requires a source full refresh or rebuild to update moved and deleted items and retrieve metadata and permission changes.</td>
</tr>
<tr>
<td>Full refresh</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Rebuild</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Document-level security</td>
<td></td>
<td>Requires the Coveo plugin for Confluence on-premises instances.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Not supported for Confluence Cloud. Permissions must be manually defined on the source.</td>
</tr>
</tbody>
</table>

9.6.2 Features

The Confluence V2 connector features are:

**Content Indexing**

Retrieval and indexing of the following Confluence item types:

- Spaces
- Pages (such as Wiki pages)
- Blog posts
- Comments (on pages and blog posts)
Note: Comments are indexed as metadata.

- Attachments (in pages, blog posts, and comments)

Fully Supported Security Model

When the Coveo plugin is installed, the connector fully supports the Confluence security model. This means that, in the Coveo search interface, a user searching Confluence content only sees the content to which he has access in Confluence.

Note: Permissions are not supported in Confluence Cloud since the required Coveo plugin cannot be installed.

Incremental Refresh

When the Coveo plugin is installed, the connector periodically queries Confluence for the latest items modifications (addition, edition, deletion), keeping the index content up-to-date.

Note: Incremental refresh is only partially supported in Confluence Cloud since the Coveo plugin cannot be installed. Therefore, without the plugin, only added and modified items (except comments) are taken into account, meaning that a full refresh or rebuild is required to update moved and deleted items and retrieve metadata and permission changes.

Pause/Resume

When indexing Confluence content, the connector can be paused and resumed.

What's Next?

Review the steps to deploy the Confluence V2 connector (see "Atlassian Confluence V2 Connector Deployment Overview" on page 789).

9.6.3 Atlassian Confluence V2 Connector Deployment Overview

The following procedure outlines the steps needed to deploy the Confluence V2 connector. The steps indicate the order in which you must perform configuration tasks on both the Confluence and Coveo servers.

To deploy the Confluence V2 connector

1. Validate that your environment meets the requirements (see "Atlassian Confluence V2 Connector Requirements" on page 791).

2. On your Confluence server:
   a. Enable the Confluence remote API.

      The Confluence V2 connector requires the Confluence SOAP remote API (Web service) to be enabled on your Confluence server (see the Atlassian document Enabling the Remote API).

   b. For an on-premises deployment, optionally install the Coveo plugin.
With Confluence on-premises installations, when you want to index permissions and perform incremental refreshes, you must install the Coveo Confluence plugin on your Confluence server (see "Installing the Coveo Plugin for Atlassian Confluence V2" on page 791).

**Notes:**
- Indexing permissions associated with each Confluence object is recommended as it allows the Coveo search interface to only show Confluence documents to which the end-user performing the search has access in Confluence.
- Because you cannot install the Coveo Confluence plugin in Confluence Cloud, Coveo cannot index permissions for this content.

3. **On the Coveo server:**
   
   a. Create a user identity.

   **Note:** When configuring the source, you must use the credentials of a native Confluence user. Users managed by other identity providers such as Google are not supported.

   - When you want to leverage the Coveo plugin to index permissions and perform incremental refreshes, with Confluence on-premises installations, you must create a user identity that refers to a Confluence administrator account (member of the confluence-administrators group) (see "Adding a User Identity" on page 420).

   - When your Confluence server does not allow anonymous users to access the REST remote API, or when you want to crawl using a specific Confluence user, you must also create a user identity and set up your Confluence V2 source to use this user identity.

   (When you do not want the user identity to be a Confluence administrator - not recommended) The following table lists the minimal required permissions that you must grant to the user identity.

   **Important:** When the user identity is not a Confluence administrator, permissions as well as pages with "View" restrictions are not indexed, and incremental refreshes are not supported (see Page Restrictions).

<table>
<thead>
<tr>
<th>Permission Type</th>
<th>Permission</th>
</tr>
</thead>
<tbody>
<tr>
<td>Global</td>
<td>Can use</td>
</tr>
<tr>
<td>Space</td>
<td>View</td>
</tr>
</tbody>
</table>

   **Note:** The user identity must have the View permission for all spaces that you want to index.

   b. Optionally create an Email security provider
When an email is defined for each of your users in Confluence and this email is used to authenticate them in your Coveo search interface, you can create an Email security provider to allow you to map your Confluence users to their email (see "Configuring an Email Security Provider" on page 65).

c. When you want to index permissions, create a security provider.

For all on-premises supported Confluence versions, when you want to index permissions, you must configure a security provider (see "Configuring an Atlassian Confluence V2 Security Provider" on page 795).

d. Create a Confluence V2 field set.

It is recommended to import the out-of-the-box Confluence V2 field set ([CES_Path]\Bin\Coveo.CES.CustomCrawlers.Confluence2.FieldSet.xml to be able to easily add Confluence-specific facets to your Coveo search interfaces.

e. Configure and index the Confluence V2 source.

The Coveo connector needs to know details about your Confluence installation to be able to index its content (see "Configuring and Indexing an Atlassian Confluence V2 Source" on page 797).

9.6.4 Atlassian Confluence V2 Connector Requirements

Your environment must meet the following requirements to be able to use the second-generation Coveo connector for Confluence:

- **CES 7.0.8225+ (March 2016)**

  The connector was introduced with the CES 7.0.8225 March 2016 release.

- Coveo license for the Confluence V2 connector

  Your Coveo license must include support for the Confluence V2 connector to be able to use this connector.

- Supported Confluence versions:
  - Confluence 6.7 to 7.1 on-premises
    - Installations using the Confluence REST API and Search REST API.
  - Confluence Cloud
    - However, document permissions and incremental refresh are not supported, because it is not possible to install the required Coveo plugin in an Atlassian Cloud instance.

What's Next?

Enable the Confluence remote API needed by the Confluence V2 connector (see the Atlassian document Enabling the Remote API).

9.6.5 Installing the Coveo Plugin for Atlassian Confluence V2

The second-generation Coveo connector for Confluence comes with a Confluence plugin. The connector needs the plugin to fully support incremental refreshes and index permissions associated with each Confluence item so that
users only see Confluence content to which they have access in Coveo search results. It is therefore recommended to install the plugin for Confluence 6.7 to 7.1 on-premises installations.

Without the plugin, you must perform a source full refresh or rebuild to take into account deleted, restored, and moved items, and items with modified comments or permissions (see Configuring and Indexing an Atlassian Confluence V2 Source). You must also set permissions globally on the source, so that all indexed Confluence content is searchable by anyone that has the permissions to view the source content (see Configuring and Indexing an Atlassian Confluence V2 Source).

**Notes:**
- The Coveo plugin cannot be installed in Confluence Cloud and consequently, permissions associated with each Confluence item cannot be indexed.
- The Coveo plugin is distributed with CES and is not available from the Atlassian Marketplace.

To install or update the Coveo Confluence Plugin

1. Log into your Confluence server using a Confluence administrator account.
2. On the top menu, access the Administration drop-down list menu by clicking the gear icon, and then select Add-ons.
3. If the Administrator Access dialog box appears, enter your administrator account credentials, and then click Confirm.
4. In the Manage add-ons page, click the Upload add-on link.
5. In the Upload add-on dialog box:
a. Click **Choose File**.

b. In the **Open** dialog box, select the \[CES_Path\]Bin\CoveoConfluenceEnhancedRestApi-\[versionNumber\].jar file from your Coveo Master server, and then click **Open**.

c. Click **Upload**.

6. In the **Installed and ready to go!** dialog box, click **Close**.
7. In the User-installed add-ons list, validate that the Coveo Enhanced REST API Plugin is listed.

To uninstall the Coveo Confluence plugin

1. Log into your Confluence server using a Confluence administrator account.
2. On the top menu, access the Administration drop-down list menu by clicking the gear icon, and then select Add-ons.
3. If the Administrator Access dialog box appears, enter your administrator account credentials, and then click Confirm.
4. In the User-installed add-ons list, locate and expand Coveo Enhanced REST API Plugin.
5. In the Coveo Enhanced REST API Plugin, click Uninstall.
6. In the Uninstall add-on? dialog box, click Uninstall add-on.

7. Validate the Coveo Enhanced REST API Plugin is no longer listed in the User-installed add-ons list.

9.6.6 Configuring an Atlassian Confluence V2 Security Provider

For an on-premises Confluence, when you installed the Coveo plugin and choose to index document permissions associated with Confluence items, the Coveo connector needs a security provider. When document permissions are indexed, in Coveo search results, a user searching for Confluence content only sees the content to which he has access in Confluence.

Note: You can get familiar with how Coveo components deal with permissions on documents both at indexing and query time.

To configure a Confluence V2 security provider

1. On the Coveo server, access the Administration Tool.


3. In the navigation panel on the left, click Security Providers.

4. In the Security Providers page, click Add to create a new security provider.

5. In the Modify Security Provider page:
a. Configure the following required parameters:

**Name**

Choose a significant name to identify the security provider.

**Example:** Confluence V2 Security Provider

**Security Provider Type**

Select Confluence v2 (x64).

**User Identity**

Select the Confluence user identity that you created previously (see "Adding a User Identity" on page 420).

**Security Provider**

Select Active Directory or a custom Active Directory security provider that you created for a specific domain to allow this Confluence security provider to map Confluence permissions to AD users.

You can select an email security provider to allow this Confluence V2 security provider to map Confluence permissions to emails. This is useful when your users are authenticated in the search interface with the same email address specified for their Confluence user, thus allowing them to also see secured documents to which they have read permissions.
Server URL

The address of the Confluence server. This should be the same address as the one that you will specify when you configure the source for the connector (see "Configuring and Indexing an Atlassian Confluence V2 Source" on page 797). Enter the URL in the following format:

http://[ConfluenceServer]:[port]

Example: http://MyConfluenceServer:8090

b. In the Parameters section, click Add Parameter to be able to change the default value of hidden parameters (see "Modifying Hidden Atlassian Confluence V2 Source Parameters" on page 804).

Note: When you implemented single sign-on Okta (CES 7.0.8691+ (December 2016)) or Atlassian Crowd SSO (CES 7.0.8850+ (March 2017) on your Confluence instance, you must add the UseRequestParametersAuth hidden parameter and set it to true both on the source and security provider configurations (see "Configuring an Atlassian Confluence V2 Security Provider" on page 795).

c. Leave the Allow Complex Identities option cleared as it does not apply to this type of security provider.

d. Click Apply Changes.

What's Next?

Configure and index a Confluence V2 source (see "Configuring and Indexing an Atlassian Confluence V2 Source" on page 797).

9.6.7 Configuring and Indexing an Atlassian Confluence V2 Source

A source defines a set of configuration parameters for a specific Confluence site.

To configure and index a Confluence V2 source

1. On the Coveo server, access the Administration Tool.

2. Select Index > Sources and Collections.

3. In the Collections section:

   a. Select an existing collection in which you want to add the new source.

   OR

   b. Click Add to create a new collection.

4. In the Sources section, click Add.

   The Add Source page that appears is organized into three sections.

5. In the General Settings section of the Add Source page:
a. Enter the appropriate value for the following required parameters:

**Name**
A descriptive name of your choice for the connector source.

**Example:** Corporate Confluence Wiki

**Source Type**
The connector used by this source. In this case, select Confluence.

**Note:** If you do not see Confluence v2 in the Source Type list, ensure that your environment meets the requirements (see "Atlassian Confluence V2 Connector Requirements" on page 791).

**Addresses**
List of starting points for the connector, one address per line.
Examples: Depending on the Confluence environment and use cases, use one of the following URL format:

- To index a complete Confluence (on-premises) site, add the Confluence server root URL:
  
  http://MyConfluenceServer:8090/

- To index specific on-premises spaces, add their URL:
  
  http://MyConfluenceServer:8090/display/space1
  http://MyConfluenceServer:8090/display/space2

- To index a complete Confluence Cloud site, add the Confluence server root URL:
  
  https://MyConfluenceServer.atlassian.net/wiki/

- To index specific Confluence Cloud spaces, add their URL:
  
  https://MyConfluenceServer.atlassian.net/wiki/display/space1
  https://MyConfluenceServer.atlassian.net/wiki/display/space2

where you replace MyConfluenceServer with your Confluence instance name, and space1 and space2 with the desired Confluence space keys.

Notes:

- To be able to index document permissions, all your starting points must be located on a single Confluence site. Create separate sources for separate sites.

- You can enter specific space addresses for deployments where Confluence is not installed at the server root, respecting the following format:
  
  http://server/MyConfluence/display/spacename.

b. The following parameters often do not need to be changed:

**Rating**

Change this value only when you want to globally change the rating associated with all items in this source relative to the rating of other sources.

**Example:** When the source indexes a legacy repository, you may want to set this parameter to Low, so that in the search interface, results from this source appear lower in the list compared to those from active repository sources.

**Document Types**

If you defined a custom document type set for this source, select it.

**Active Languages**

If you defined custom active language sets, ensure to select the most appropriate for this source.
Fields

Select the field set that you created earlier (see Atlassian Confluence V2 Connector Deployment Overview).

Refresh Schedule

Time interval at which the index is automatically refreshed to keep the index content up-to-date. By default, the Every day option instructs CES to refresh the source everyday at 12 AM. Because the incremental refresh (supported when the plugin is installed) takes care of maintaining the source up-to-date, you can select a longer interval such as Every Sunday.

6. In the Specific Connector Parameters & Options section of the Add Source page:

   a. Review if you need to change the default values for the following parameters:

      Filter Space Regex

      The regex to use to filter spaces when you want to index only a subset of Confluence.

      **Note:** This parameter is useful when you have a large number of spaces to index that have an element in common in their space keys.

      **Example:** You want to index all spaces with keys starting with an uppercase letter followed by a number, so you enter the following regex:

         \^[A-Z] [0-9].*$

      Number of Refresh Threads

      Determines the number of refresh threads that allow the connector to crawl web pages in parallel. The default value is 2 threads.
**Note:** Increasing this value may improve source refresh speed but puts more load on the Confluence server.

**Mapping File**

The path to the mapping file that defines how the connector handles metadata. Leave the default value to use the default mapping file that comes with the connector (Coveo.CES.CustomCrawlers.Confluence2.MappingFile.xml). If you create a custom mapping file, enter the full path to your custom mapping file. Contact Coveo Support for assistance if you need to customize the mapping file.

**Index Only Global Spaces**

When selected, only global spaces are indexed, meaning that personal spaces are ignored.

**Index Only Personal Spaces**

When selected, only personal spaces are indexed, meaning that global spaces are ignored.

**Index Comments**

When selected, comments on blog posts and pages are indexed. Comments are indexed as metadata of the page, not as documents.

**Index Attachments**

When selected, binary files attached to a page, blog post or comment are indexed. Attachments are indexed with the same level and sets of their parent.

b. Review the **Option** check boxes generally do not need to be changed:

**Index Subfolders**

Keep this check box selected (recommended). By doing so, all subfolders from the specified server address are indexed.

**Index the document’s metadata**

When selected, CES indexes all the document metadata, even metadata that are not associated with a field. The orphan metadata are added to the body of the document so that they can be searched using free text queries.

When cleared (default), only the values of system and custom fields that have the **Free Text Queries** attribute selected will be searchable without using a field query.
Example: A document has two metadata:

- LastEditedBy containing the value Hector Smith
- Department containing the value RH

In CES, the custom field CorpDepartment is bound to the metadata Department and its Free Text Queries attribute is selected.

When the Index the document's metadata option is cleared, searching for RH returns the document because a field is indexing this value. Searching for hector does not return the document because no field is indexing this value.

When the Index the document's metadata option is selected, searching for hector also returns the document because CES indexed orphan metadata.

Document's addresses are case-sensitive

Leave the check box cleared. This parameter needs to be checked only in rare cases for systems in which distinct documents may have the same name but different casing.

Generate a cached HTML version of indexed documents

When you select this check box (recommended), at indexing time, CES creates HTML versions of indexed documents. In the search interfaces, users can then more rapidly review the content by clicking the Quick View link rather than opening the original document with the original application. Consider clearing this check box only when you do not want to use Quick View links or to save resources when building the source.

Open results with cached version

Leave this check box cleared (recommended) so that in the search interfaces, the main search result link opens the original document with the original application. Consider selecting this check box only when you do not want users to be able to open the original document but only see the cached HTML version of the document as a Quick View. In this case, you must also select Generate a cached HTML version of indexed documents.

c. In the Parameters section, click Add Parameter to be able to change the default value of hidden parameters (see "Modifying Hidden Atlassian Confluence V2 Source Parameters" on page 804).

Note: When you implemented single sign-on Okta (CES 7.0.8691+ (December 2016)) or Atlassian Crowd SSO (CES 7.0.8850+ (March 2017) on your Confluence instance, you must add the UseRequestParametersAuth hidden parameter and set it to true both on the source and security provider configurations (see "Configuring an Atlassian Confluence V2 Security Provider" on page 795).

7. In the Security section of the Add Source page:
a. In the Authentication drop-down list, if you chose to index permissions, select the Confluence crawling user identity that you created for this source. Otherwise, select None.

b. In the Security Provider drop-down list, if you chose to index permissions, select the Confluence security provider that you created for this source (see "Configuring an Atlassian Confluence V2 Security Provider" on page 795). Otherwise, select None.

**Note:** When you select None, in the Authentication and Security Provider drop-downs, only your public (unsecured) Confluence content will be indexed.

c. Click Save and Start to save the source configuration and build the source.

8. When you chose to NOT index permissions, you must set the permissions globally for the source:
a. In the navigation menu on the left, select **Permissions**.

b. Next to **Permissions**, select the **Specifies the security permissions to index** option.

c. Next to **Allowed Users**, ensure that a well-known everyone group such as the Active Directory S-1-1-0 is added.

d. Click **Apply Changes**.

9. Validate that the source building process is executed without errors:

   - In the navigation panel on the left, click **Status**, and then validate that the indexing proceeds without errors.

   OR

   - Open the CES Console to monitor the source building activities.

9.6.8 Modifying Hidden Atlassian Confluence V2 Source Parameters

The **Add Source** and **Source: ... General** pages of the Administration Tool present the parameters with which you can configure the connector for most Confluence setups. More advanced and more rarely used parameters are hidden. You can choose to make one or more of these parameters appear in the **Add Source** and **Source: ... General** pages of the Administration Tool so that you can change their default value. Consider changing values of hidden parameters when you encounter issues.
The following list describes the advanced hidden parameters available with Confluence V2 sources. The parameter type (integer, string,...) appears between parentheses following the parameter name.

IndexArchivedSpaces (Boolean) CES 7.0.8996+ (June 2017)
Whether to retrieve the content of archived spaces. The default value is True.

IndexCurrentSpaces (Boolean) CES 7.0.8996+ (June 2017)
Whether to retrieve the content of active (unarchived) spaces. The default value is True.

IndexSpaces (Boolean) CES 7.0.9167+ (December 2017)
Whether to index spaces (the entities, not the space content) as separate documents. The default value is True.

SpacesBatchSize (Integer)
The number of spaces to retrieve with each call to the REST API (between 1 and 500). The default value is 50.

ContentItemsBatchSize (Integer)
The number of content items to retrieve with each call to the REST API (between 1 and 100). The default value is 50.

UseRequestParametersAuth (Boolean) Security provider
Whether to use request parameters os_username and os_password instead of the HTTP basic authentication via standard HTTP headers. The default value is False. Set to True when you use cookie (form-based) authentication (e.g., Okta single-sign on).

Note: CES 7.0.8691+ (December 2016) The Coveo plugin works with single sign-ons such as Okta when the UseRequestParametersAuth parameter is set to true (see "Installing the Coveo Plugin for Atlassian Confluence V2" on page 791).

NumberOfRetries (Integer)
The maximum number of times a failing request is retried. The default value is 5 retries.

RequestTimeout (Integer)
The maximum amount of time in seconds a request can be executed before being canceled. The default value is 100 seconds.

ActiveDirectoryDomainNameForMappings (String) Security provider
(When your Confluence usernames are the same as the ones in your Active Directory) The Active Directory domain name used to map Confluence permissions to AD identities.

Example: When you enter TechnoWiki as your company domain, every username will be mapped like the following when permissions are resolved:

TechnoWiki\username

Use the following procedure only when you want to modify one or more of the above hidden source parameters.
To modify hidden Confluence V2 source parameters

1. Refer to "Adding an Explicit Connector Parameter" on page 450 to add one or more Confluence V2 hidden source parameters.

2. For a new Confluence V2 source, access the Add Source page of the Administration Tool to modify the value of the newly added advanced parameter:
   a. Select Index > Sources and Collections.
   b. Under Collections, select the collection in which you want to add the source.
   c. Under Sources, click Add.
   d. In the Add Source page, edit the newly added advanced parameter value.

3. For an existing Confluence V2 source, access the Source: ... General page of the Administration Tool to modify the value of the newly added advanced parameter:
   a. Select Index > Sources and Collections.
   b. Under Collections, select the collection containing the source you want to modify.
   c. Under Sources, click the existing Confluence V2 source in which you want to modify the newly added advanced parameter.
   d. In the Source: ... General page, edit the newly added advanced parameter value.

4. Rebuild your Confluence V2 source to apply the changes to the parameters.

9.7 Atlassian Jira Software V2 Connector

 CES 7.0.7104+ (October 2014)

The second generation (V2) Coveo connector for Jira Software allows you to index and integrate the content of your Jira Software instance into your Coveo unified index, making it easily searchable by end-users.

9.7.1 Connector Features Summary

<table>
<thead>
<tr>
<th>Features</th>
<th>Supported</th>
<th>Additional information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Jira Software version</td>
<td>6.1 to 7.1.2 and Cloud</td>
<td></td>
</tr>
<tr>
<td>Searchable content types</td>
<td>✔️ Projects¹, issues, comments, attachments, and work logs</td>
<td></td>
</tr>
</tbody>
</table>

¹ Additional features available in the CES 7.0.7104+ (October 2014) release.
### 9.7.2 Features

- **Content Indexing**
  
  Retrieval and indexing of the following Jira Software repository items:
  
  - Projects
  
    **Note:** Project metadata is indexed on the issues of the project, but the projects themselves are not indexed.
  
  - Issues
  
  - Comments
  
  - Attachments
  
  - Work Logs

- **Security**

  The connector supports the Jira security model by indexing Jira item permissions so that in Coveo search interfaces, a user searching Jira content only sees the content to which he has access in Jira.

  As shown in the following table, you can index all Jira Software permission types with the Coveo plugin (see "Installing the Coveo Plugin for Atlassian Jira Software" on page 814), except for Jira Software Cloud, because it is not possible to install plugins in cloud instances. Starting with Jira Software 7, a new Atlassian API allows the Coveo connector to index most permissions without the need of a plugin.

<table>
<thead>
<tr>
<th>Features</th>
<th>Supported</th>
<th>Additional information</th>
</tr>
</thead>
</table>
| **Content update**| Incremental refresh | CES 7.0.9093+ (September 2017) A source rebuild is required to retrieve:  
  - Changes (creation, edition, deletion) on projects  
  - Deletion of issues  
  The source can receive push notifications from a Jira webhook following any change of Jira content, allowing to keep the source content up-to-date (see "Creating a Jira Software Webhook" on page 810). |
|                   | Full refresh |  
|                   | Rebuild     |  
| **Document-level security** |  
|                   |  
|                   | ✓          | Requires the Coveo plugin for Jira Software (self-hosted) instances.  
|                   | ✓          | Not supported for Jira Cloud. Permissions must be manually defined on the source. [more] |
### Supported permission types

<table>
<thead>
<tr>
<th>Supported permission types</th>
<th>With plugin</th>
<th>Without plugin</th>
</tr>
</thead>
<tbody>
<tr>
<td>Group &amp; user</td>
<td>6.x, 7+</td>
<td>7+</td>
</tr>
<tr>
<td>Project</td>
<td>6.x, 7+</td>
<td>7+</td>
</tr>
<tr>
<td>Application role</td>
<td>6.x, 7+</td>
<td>7+</td>
</tr>
<tr>
<td>Issue-level</td>
<td>6.x, 7+</td>
<td></td>
</tr>
<tr>
<td>Attachments</td>
<td>6.x, 7+</td>
<td>7+</td>
</tr>
<tr>
<td>Comments</td>
<td>6.x, 7+</td>
<td>7+</td>
</tr>
<tr>
<td>Time Tracking</td>
<td>6.x, 7+</td>
<td>7+</td>
</tr>
<tr>
<td>CES 7.0.8541+ (September 2016)</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

- **Live monitoring**

  The connector receives push notifications from a Jira webhook following any change of Jira content, allowing to keep the index up-to-date (see Creating a Jira Software Webhook).

- **Incremental Refresh CES 7.0.9093+ (September 2017)**

  The connector periodically queries Jira Software for the latest items modifications (addition, edition, deletion), keeping the index content up-to-date.

  **Note:** A full refresh or rebuild is required to retrieve:

  - Changes (creation, edition, deletion) on projects
  - Deletion of issues

### What's Next?

Get familiar with the connector deployment steps (see "Atlassian Jira Software V2 Connector Deployment Overview" on page 808).

#### 9.7.3 Atlassian Jira Software V2 Connector Deployment Overview

The following procedure outlines the steps needed to deploy the Jira Software V2 connector. The steps indicate the order in which you must perform configuration tasks on both the Jira Software and Coveo servers.

To deploy the Jira Software V2 connector

1. Validate that your environment meets the requirements (see "Atlassian Jira V2 Connector Requirements" on page 810).
2. On your Jira Software (self-hosted) server or Jira Software Cloud instance:
a. Create a webhook (see “Creating a Jira Software Webhook” on page 810).

b. Optionally, install the Coveo plugin.

When you want to index permissions, you must install the Coveo Jira Software V2 plugin on your Jira Software (self-hosted) server (see “Installing the Coveo Plugin for Atlassian Jira Software” on page 814).

Unless you are only indexing anonymously accessible content, it is recommended to index permissions to allow Coveo search interfaces to only show Jira Software documents to which the end-user performing the search has access in Jira.

Note: Because you cannot add plugins to Jira Software Cloud, it is not possible to index Jira Software Cloud item permissions.

3. On the Coveo server:

a. Create a user identity.

The connector will only index issues to which the crawling user identity is granted access to. This means the Jira Software user account used as the crawling user identity must first be assigned to all necessary Jira permission schemes required in order to gain access to the issues to index.

Notes:

- When configuring the source, you must use the credentials of a native Jira Software user. Users managed by other identity providers such as Google are not supported.
- If the crawling user identity is only granted access to a subset of the Jira Software projects, only issues from these projects will be indexed.

When you want to index permissions, you must also grant Jira Administrators global permission to this user identity.

Tip: CES 7.0.8225+ (March 2016) If you want to only index public documents, simply create a user identity with any credentials. The connector must have a non-empty user identity.

b. CES 7.0.7814+ (August 2015) Optionally create an Email security provider

When an email is defined for each of your users in Jira Software and this email is used to authenticate them in your Coveo search interface, you can create an Email security provider to allow you to map your Jira Software users to their email (see “Configuring an Email Security Provider” on page 65).

c. Create a security provider.

When you want to index permissions, you must configure a security provider (see “Configuring an Atlassian Jira Software V2 Security Provider” on page 817).

d. Create a Jira Software V2 field set.

It is recommended to import the out-of-the-box Jira V2 field set (\CES_Path\Bin\Coveo.CES.CustomCrawlers.Jira2.FieldSet.xml) to be able to easily add Jira specific facets to your Coveo search interfaces.
e. Configure and index the Jira Software V2 source.

The Coveo connector needs to know details about your Jira Software instance to be able to index its content (see "Configuring and Indexing an Atlassian Jira Software V2 Source" on page 820).

9.7.4 Atlassian Jira V2 Connector Requirements

Your environment must meet the following requirements to be able to use the Coveo connector for Jira Software V2:

- **CES 7.0.7104+ (October 2014)**
- Coveo license for the Jira Software V2 connector
  
  Your Coveo license must include support for the Jira Software V2 connector to be able to use this connector.

- Jira Software versions:
  - Supported versions:
    - Cloud
    - 6.1 to 7.1.2 (self-hosted)
  - **Note:** CES 7.0.8541+ (September 2016) Support for Jira Software (self-hosted) v7.0 to 7.1.2
  - Deprecated support versions: 5.2 to 6.0 (self-hosted)

What’s Next?

On your Jira Software (self-hosted) server:

- Create a webhook to allow your source to perform live monitoring of your Jira Software instance (see Creating a Jira Software Webhook).
- Install the Coveo plugin to be able to index Jira Software security permissions (see "Installing the Coveo Plugin for Atlassian Jira Software" on page 814).

9.7.5 Creating a Jira Software Webhook

The webhook pushes notifications for any change in Jira content, allowing the connector to immediately index new, modified, or deleted items. The following procedure outlines the steps needed to deploy Jira Software webhooks on the Jira Software server (see Managing Webhooks and Webhooks).

To create a Jira Software Webhook

1. Log in to your Jira instance using an account with the **Jira Administrator global permission** (see Managing Global Permissions).

2. Access the Webhooks page:

   a. In the top-right menu, in the gear drop-down list, select **System**.

   b. In the **Administrator Access** box, enter your password, and then click **Confirm**.
c. In the system **Settings** page, in the navigation bar on the left, under **Advanced**, select **Webhooks**.

3. In the **Webhooks** page, click **Create a Webhook** icon.

4. Create the webhook using the parameters and default values shown in the following table:

<table>
<thead>
<tr>
<th>Parameter name</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Significant name of your choice (e.g. Jira Software Webhook)</td>
</tr>
<tr>
<td>URL</td>
<td>http://[YourCoveoMasterServer]/jira/CoveoCrawler/JiraWebHook</td>
</tr>
</tbody>
</table>

**Important:** Once you enable the webhook, it sends data each time an event occurred in Jira Software. If you use an unsecured HTTP webhook, be aware that it can expose potentially sensitive information. It is thus strongly recommended to set an HTTPS webhook instead (see [HTTPS webhook](https://www.coveo.com)).

**Note:** CES 7.0.7183+ (November 2014) Setting an HTTPS webhook support.

<table>
<thead>
<tr>
<th>Events</th>
<th>All issue events</th>
</tr>
</thead>
</table>

**Note:** CES 7.0.8541+ (September 2016) For Jira Software (self-hosted) 7, only select the checkboxes under **Issue**.

**Important:** If the **Exclude details** check box is selected, your Jira Software permissions will not be updated. Leave the check box cleared.
5. Click Create.
Notes:

- By default, the live monitoring feature listens on the http:// [YourCoveoMasterServer]/jira/CoveoCrawler/JiraWebHook web service endpoint.

  **Important:** Once you enable the webhook, it sends data each time an event occurred in Jira Software. If you use an unsecured HTTP webhook, be aware that it can expose potentially sensitive information. It is thus strongly recommended to set an HTTPS webhook instead (see HTTPS webhook).

  **Note:** CES 7.0.7183+ (November 2014) Support for setting an HTTPS webhook.

- If you have more than one Jira Software V2 source, create a webhook for each of your Jira Software V2 source by using the WebServiceEndpointName hidden parameter to replace the web service endpoint name (CoveoCrawler part) in the default web service endpoint URL (http://CoveoMasterServer/jira/CoveoCrawler/JiraWebHook).

  **Example:** When the WebServiceEndpointName hidden parameter value is changed to CoveoCrawler1, the web service endpoint URL becomes http://CoveoMasterServer/jira/CoveoCrawler1/JiraWebHook. You can then create another webhook using this URL.

- By default, live monitoring is enabled on a Jira Software V2 source. If you disable live monitoring, your source will not be updated other than with the full refreshes.

  **CES 7.0.7183+ (November 2014)** You can set the exposed secured endpoint to use an https connection between the Jira webhook and the crawler endpoint.

  - On a normal setup:
    - a. Set the parameter WebServiceEndpointUseHttps to true (see Modifying Hidden Atlassian Jira Software V2 Source Parameters).
    - b. Configure the port 443 with the ssl certificate. You can use the command `netsh http add sslcert ipport=0.0.0.0:443 certhash=[tumbprint] appid=\{\{crawler appid\}\}` (see How to: Configure a Port with an SSL Certificate).
    - c. When you use self-signed certificate, you must export the certificate in Base64 from the machine where the Coveo Master server is located and add it into the Java KeyStore of Jira:
      - On the machine where Coveo Master server is located:
        - a. Open Internet Information Services (IIS) manager.
        - b. Under Connections, click the server name, and then Server Certificates.
        - c. Select the good certificate, and then under Actions, select View.
        - d. On the Details tab, click Copy to File.
        - e. In the Welcome to the Certificate Export Wizard window, read, and then click Next.
        - f. In the Export Private Key window, select the No, do not export the private key check box, and
then click Next.

g. In the Export File Format window, select the Base-64 encoded X.509 (.CER) check box, and then click Next.

h. In the File to Export window, in the File Name box, enter the name of the certificate you want to export.

By default, the file is saved in the C:\windows\system32\ folder.

i. In the Completing the Certificate Export Wizard window, click Finish.

n On the Jira Software machine:

a. Open Command Prompt.

b. Run the following command to import the certificate into the Java KeyStore:

   %JAVA_HOME%\bin\keytool -import -alias jira_tomcat -file [Your_Certificate_Path].CER -keystore %JAVA_HOME%\jre\lib\security\cacerts

c. Enter changeit, the default Java TrustStore password, when asked for a password.

If you try to setup an HTTPS webhook with a self-signed certificate and encountered problems, refer to the Jira documentation (see SSLHandshakeException - unable to find valid certification path to requested target).

What’s Next?

On your Jira Software (self-hosted) server, install the Coveo plugin to be able to index Jira Software security permissions (see "Installing the Coveo Plugin for Atlassian Jira Software" on page 814).

9.7.6 Installing the Coveo Plugin for Atlassian Jira Software

The Coveo connector for Jira Software V2 comes with a Jira Software plugin. When you want to index Jira Software permissions, you must install this plugin on your Jira Software (self-hosted) server.

Notes:

- Because you cannot add plugins to Jira Software on Atlassian Cloud, it is not possible to index Jira Software Cloud item permissions.

- When you upgrade CES to a version that contains an updated Jira Software plugin, you must uninstall the old plugin and reinstall the new one. If you do not, you will see an error message similar to the following one:

The version [n] of Coveo Enhanced REST API is not supported. The minimal required version is [m].

To install the Coveo Jira Software Plugin

1. From the Coveo Master server, copy the Coveo plugin file ([Index_Path]\Bin\CoveoEnhancedRestApi.jar) and paste it to a location and computer of your choice accessible to the browser that you will use to install the plugin from the Jira Software Manage Add-on page.
2. Log into your Jira Software (self-hosted) server using a Jira Software administrator account.

3. On the menu, click Browse > Add-ons.

4. If the Administrator Access dialog box appears, enter your administrator account credentials, and then click Confirm.

5. In the navigation panel on the left, under Atlassian Marketplace, click Manage Add-ons.

6. In the Manage Add-ons page, click the Upload add-on link.

7. In the Upload add-on dialog box:
   a. Click Choose File.
   b. In the Open dialog box, select the Coveo plugin file that you copied on step 1, and then click Open.
   c. Click Upload.

8. In the Installed and ready to go! dialog box, click Close.
9. In the User-installed Add-ons list, validate that the Coveo Enhanced REST API Plugin is listed.

To uninstall the Coveo Jira plugin

1. Log into your Jira Software (self-hosted) server using a Jira Software administrator account.
2. On the menu, click Browse > Add-ons.
3. If the Administrator Access dialog box appears, enter your administrator account credentials, and then click Confirm.
4. In the navigation panel on the left, under Atlassian Marketplace, click Manage Add-ons.
5. In the User-installed Add-ons list, locate and expand Coveo Enhanced REST API Plugin.
6. In the Coveo Enhanced REST API Plugin, click Uninstall.
7. In the Confirm dialog box, click Continue.

8. Validate the Coveo Enhanced REST API Plugin is no longer listed in the User-installed Add-ons list.

9.7.7 Configuring an Atlassian Jira Software V2 Security Provider

When you choose to index permissions associated with Jira Software items, the Coveo connector needs a security provider. When permissions are indexed, in Coveo search results, a user searching for Jira Software content only sees the content to which he has access in Jira.

**Note:** You can get familiar with how Coveo components deal with permissions on documents both at indexing and query time.

To configure a Jira Software V2 security provider

1. On the Coveo server, access the Administration Tool.
3. In the navigation panel on the left, click Security Providers.
4. In the Security Providers page, click Add to create a new security provider.
5. In the Modify Security Provider page:
a. Configure the following required parameters:

**Name**

Choose a significant name to identify the security provider.

**Example:** Jira Software V2 Security Provider

**Security Provider Type**

Select Jira v2 (x64).

**User Identity**

Select the Jira Software V2 user identity that you created previously.

**Jira Web Service URL**

Enter the address of your Jira Software (self-hosted) server. This should be the same address as the one you will also enter in the Addresses parameter of your source (see "Configuring and Indexing an Atlassian Jira Software V2 Source" on page 820). Enter your Jira Software server URL in the following format:

http://[JiraSoftwareServer]:[port]
**Security Provider**

Select another security provider to allow the Jira Software security provider to map Jira Software accounts to another user type with which people are authenticated when they perform a search:

- When the Jira Software LDAP is synchronized with an Active Directory, select the out-of-the-box **Active Directory** security provider to map Jira Software users to AD users.

- **CES 7.0.7814+ (August 2015)** When an email is defined for all users in Jira Software and they are authenticated with this email when they perform a search in your CES search interface, select the Email security provider you previously created (see Atlassian Jira Software V2 Connector Deployment Overview).

**Note: CES 7.0.7711– (June 2015)** If your Jira and AD user names do not match, contact Coveo Support for assistance with other methods to map users.

<table>
<thead>
<tr>
<th>b.</th>
<th>(Optional) Select the <strong>Expand 'any logged in user' Virtual Group</strong> check box when you want the <strong>any logged in user</strong> virtual group to contain all your Jira Software users.</th>
</tr>
</thead>
</table>

**Notes:**

- Inactive users are not expanded even when the option is selected.

- By default, the **any logged in user** virtual group only contains the Jira Software users seen by the Coveo security provider.

<table>
<thead>
<tr>
<th>c.</th>
<th>(Optional) In the <strong>Parameters</strong> section, click <strong>Add Parameter</strong> and then use the following hidden parameters when you want to use Kerberos authentication:</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Name</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td><strong>UseKerberosAuthentication</strong></td>
<td>true</td>
</tr>
<tr>
<td></td>
<td><strong>ServicePrincipalNames</strong></td>
<td>HTTP/server.name@server.domain</td>
</tr>
<tr>
<td></td>
<td></td>
<td><img src="image" alt="Delete" /></td>
</tr>
<tr>
<td></td>
<td><img src="image" alt="Add Parameter" /></td>
<td><img src="image" alt="Add Parameter" /></td>
</tr>
</tbody>
</table>

**UseKerberosAuthentication** **Source CES 7.0.7711+ (June 2015)**

Whether to use Kerberos authentication. The default value is **false**. Set it to **true** when crawling a Kerberos setup.

**ServicePrincipalNames** **Source CES 7.0.7711+ (June 2015)**

The custom server principal name (SPN) to use with the Kerberos authentication. The SPN is almost always in the following format: `HTTP/server.name@server.domain`. If the domain name is not contained in the SPN, the connector uses the user domain, which may be wrong. Use this parameter when the crawling user identity used is not on the same domain as the Jira Software server.

**Example:** You use **user@domain.com** as the user identity to crawl **http://jira.dev.domain.com**.
Notes:

- This parameter is only used when the UseKerberosAuthentication parameter value is true.
- Make sure the user identity exists in both Jira Software and AD.
- When you get the following error:
  
  The Kerberos Authentication failed for user 'userIdentity' with the SPN 'HTTP/ServerName'.

  it means the user identity and/or the SPN are wrong.

  d. Leave the Allow Complex Identities cleared as it does not apply to this type of security provider.
  
  e. Click Apply Changes.

What's Next?

Configure and index a Jira Software V2 source (see "Configuring and Indexing an Atlassian Jira Software V2 Source" on page 820).

9.7.8 Configuring and Indexing an Atlassian Jira Software V2 Source

A source defines a set of configuration parameters for a specific Jira Software instance.

To configure and index a Jira Software V2 source

1. On the Coveo server, access the Administration Tool.
2. Select Index > Sources and Collections.
3. In the Collections section:
   a. Select an existing collection in which you want to add the new source.
      OR
   b. Click Add to create a new collection.
4. In the Sources section, click Add.
   The Add Source page that appears is organized in three sections.
5. In the General Settings section of the Add Source page:
a. Enter the appropriate value for the following required parameters:

**Name**

A descriptive name of your choice for the connector source.

**Example:** `Jira V2`

**Source Type**

The connector used by this source. In this case, select `Jira v2`.

**Note:** If you do not see `Jira v2` in the **Source Type** list, ensure that your environment meets the requirements (see "Atlassian Jira V2 Connector Requirements" on page 810).

**Addresses**

Enter the base URL of your Jira Software server.

**Example:** `http://MyJiraServer:8080/`

**Fields**

Select the field set that you created earlier (see Atlassian Jira Software V2 Connector Deployment Overview).
b. The following parameters often do not need to be changed:

**Rating**

Change this value only when you want to globally change the rating associated with all items in this source relative to the rating of other sources.

**Example:** When the source indexes a legacy repository, you may want to set this parameter to Low, so that in the search interface, results from this source appear lower in the list compared to those from active repository sources.

**Document Types**

If you defined a custom document type set for this source, select it.

**Active Languages**

If you defined custom active language sets, ensure to select the most appropriate for this source.

**Refresh Schedule**

Time interval at which the index is automatically refreshed to keep the index content up-to-date. By default, the *Every day* option instructs CES to refresh the source everyday at 12 AM.

Live monitoring with a Jira webhook efficiently and continuously maintains your source up to date. The full refresh is a safety net to ensure all modifications are taken into account.

**Example:** If your Coveo Master Server is down for maintenance for an hour and the Jira webhook pushes changes during that time, they will only be taken into account in the index on the next full refresh.

6. In the **Specific Connector Parameters & Options** section of the **Add Source** page:
a. In the **Mapping File** box, the path to the default mapping file that defines how the connector handles metadata often does not need to be changed.

b. Review if you need to change the default values for the following parameters:

**Support Comment Permissions**

By default, this check box is cleared so the issue and its comments are indexed as one document, allowing to find a document from either an issue or its comments. However, there are no restrictions on users seeing comments on an issue.

Select the check box, to respect the permissions on the comments, so that only users allowed to see a comment in Jira Software can also see it in search results. In this case, an issue and its comments are indexed in separate documents leading to lower search relevance.

**Index Attachments**

When selected, CES indexes binary files attached to an issue. Attachments are indexed with the same level and sets of their parent issue.

**Index Comments**

When selected, CES indexes comments on issues. Comments are indexed with the same level and sets of their parent issue. When permissions on the comments are supported, if a comment is restricted to a group or a project role, an additional set with the group or the role is added.

**Index Work Logs**

When selected, CES indexes time entry on an issue. Work logs are indexed with the same level and sets of their parent issue. If a work log is restricted to a group or a project role, an additional set with the group or the role is added.

c. (Optional) In the **Parameters** section, click **Add Parameter** and then use the following hidden parameters when you want to use Kerberos authentication:

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>UseKerberosAuthentication</td>
<td>true</td>
</tr>
<tr>
<td>ServicePrincipalNames</td>
<td>HTTP/server.name@server.domain</td>
</tr>
</tbody>
</table>

**UseKerberosAuthentication**  

Whether to use Kerberos authentication. The default value is *false*. Set it to *true* when crawling a Kerberos setup.

**ServicePrincipalNames**  

The custom server principal name (SPN) to use with the Kerberos authentication. The SPN is almost always in the following format: `HTTP/server.name@server.domain`. If the domain name is not contained in the SPN, the connector uses the user domain, which may be wrong. Use this parameter when the crawling user identity used is not on the same domain as the Jira Software server.
Example: You use user@domain.com as the user identity to crawl http://jira.dev.domain.com.

Notes:
- This parameter is only used when the UseKerberosAuthentication parameter value is true.
- Make sure the user identity exists in both Jira Software and AD.
- When you get the following error:
  The Kerberos Authentication failed for user 'userIdentity' with the SPN 'HTTP/ServerName'.
  it means the user identity and/or the SPN are wrong.

d. The Option check boxes generally do not need to be changed:

Index Subfolders

Keep this check box selected (recommended). By doing so, all subfolders from the specified server address are indexed.

Index the document's metadata

When selected, CES indexes all the document metadata, even metadata that are not associated with a field. The orphan metadata are added to the body of the document so that they can be searched using free text queries.

When cleared (default), only the values of system and custom fields that have the Free Text Queries attribute selected will be searchable without using a field query.

Example: A document has two metadata:
- LastEditedBy containing the value Hector Smith
- Department containing the value RH

In CES, the custom field CorpDepartment is bound to the metadata Department and its Free Text Queries attribute is selected.

When the Index the document's metadata option is cleared, searching for RH returns the document because a field is indexing this value. Searching for hector does not return the document because no field is indexing this value.

When the Index the document's metadata option is selected, searching for hector also returns the document because CES indexed orphan metadata.

Document's addresses are case-sensitive

Leave the check box cleared. This parameter needs to be checked only in rare cases for systems in which distinct documents may have the same name but different casing.

Generate a cached HTML version of indexed documents

When you select this check box (recommended), at indexing time, CES creates HTML versions of
indexed documents. In the search interfaces, users can then more rapidly review the content by clicking the Quick View link rather than opening the original document with the original application. Consider clearing this check box only when you do not want to use Quick View links or to save resources when building the source.

**Open results with cached version**

Leave this check box cleared (recommended) so that in the search interfaces, the main search result link opens the original document with the original application. Consider selecting this check box only when you do not want users to be able to open the original document but only see the HTML version of the document as a Quick View. In this case, you must also select **Generate a cached HTML version of indexed documents**.

7. **In the Security section of the Add Source page:**

   ![Security section](image)

   a. In the **Authentication** drop-down list, select the Jira Software V2 crawling user identity that you created for this source (see Atlassian Jira Software V2 Connector Deployment Overview).

   b. In the **Security Provider** drop-down list, if you chose to index permissions, select the Jira Software V2 security provider that you created for this source (see "Configuring an Atlassian Jira Software V2 Security Provider" on page 817). Otherwise, select **None**.

   c. Click **Save** to save the source configuration.

8. **In the case your Jira content is all public and you chose to not index Jira permissions:**
a. In the navigation menu on the left, select **Permissions**.

b. Next to **Permissions**, select the **Specifies the security permissions to index** option.

c. Next to **Allowed Users**, ensure that a well-known everyone group such as the Active Directory `everyone \S-1-1-0\` is added.

d. Click **Apply Changes**.

9. On the toolbar, click **Rebuild** to start indexing your source.

10. Validate that the source building process is executed without errors:

    a. In the navigation panel on the left, click **Status**, and then validate that the indexing proceeds without errors.

    OR

    b. Open the CES Console to monitor the source building activities.
What's Next?

Consider modifying advanced source parameters (see "Modifying Hidden Atlassian Jira Software V2 Source Parameters" on page 827).

9.7.8.1 Modifying Hidden Atlassian Jira Software V2 Source Parameters

The **Add Source** and **Source: ... General** pages of the Administration Tool present the parameters with which you can configure the connector for most Jira setups. More advanced and more rarely used parameters are hidden. You can choose to make one or more of these parameters appear in the **Add Source** and **Source: ... General** pages of the Administration Tool so that you can change their default value. Consider changing values of hidden parameters when you encounter issues.

The following list describes the advanced hidden parameters available with Jira Software V2 sources. The parameter type (integer, string…) appears between parentheses following the parameter name.

**NumberOfRefreshThreads (Integer)**

Determines the number of threads used while indexing Jira Software documents. The default and recommended value is 2.

**BatchSize (Integer)**

Number of items to retrieve with each call to the web service. The default and recommended value is 100.

**WebServiceEndpointUrl (String)**

The point of contact on the Coveo Master server where a Jira Software webhook can send information to. When you have a particular setup that requires a specific endpoint, use this parameter to completely override the default web service endpoint URL (http://[CoveoMasterServer]/jira/CoveoCrawler/JiraWebHook). CES appends /JiraWebhook to the end of the parameter value.

**Example:** When you change the **WebServiceEndpointURL** value to http://111.111.111.111, your webhook must use this URL: http://111.111.111.111/JiraWebhook (see Creating a Jira Software Webhook).

**WebServiceEndpointName (String)**

Name of the CES Jira Software web service endpoint for Jira Software webhooks. The default value is CoveoCrawler. When you have more than one Jira Software V2 source using the live monitoring feature, change the value of this parameter to replace the CoveoCrawler part of the default web service endpoint URL (http://[CoveoMasterServer]/jira/CoveoCrawler/JiraWebHook).

**Examples:**

- When you change the **WebServiceEndpointName** value to CoveoCrawler1, the web service endpoint URL that you specify in the Jira Software webhook becomes http://[CoveoMasterServer]/jira/CoveoCrawler1/JiraWebHook

- When you change the **WebServiceEndpointName** value to SecondCoveoCrawler, the web service endpoint URL that you specify in the Jira Software webhook becomes http://[CoveoMasterServer]/jira/SecondCoveoCrawler/JiraWebHook.
WebServiceEndpointUseHttps (Boolean) CES 7.0.7183+ (November 2014)

Whether the exposed secured endpoint uses an https connection between the Jira Software webhook and the crawler endpoint. The default value is false. Change the value to true when you want to make the endpoint web service endpoint secured by HTTPS.

Example: When the parameter value is set to true, the web service endpoint URL uses an https connection (https://[CoveoMasterServer]/jira/CoveoCrawler/JiraWebHook).

RetrieveThumbnails (Boolean)

Whether to retrieve thumbnails of attachments. The default value is true. However, it is not recommended to use this parameter if it does not add value to your search interface. Retrieving thumbnails takes disk space and can slow down source indexing time depending on your source size.

WebInterfaceRootUrl (String)

The URL to the Jira Software web interface containing /browse. Use that parameter when your clickable URL does not work.

Note: All item URLs must be in the http://[MyJiraServer]:[port]/browse/[ItemKey] form to work.

UseKerberosAuthentication (Boolean) Security provider CES 7.0.7711+ (June 2015)

Whether to use Kerberos authentication. The default value is false. Set it to true when crawling a Kerberos setup.

ServicePrincipalNames (String) Security provider CES 7.0.7711+ (June 2015)

The custom server principal name (SPN) to use with the Kerberos authentication. The SPN is almost always in the following format HTTP/server.name@server.domain. If the domain name is not contained in the SPN, the connector uses the user domain, which may be wrong. Use this parameter when the crawling user identity used is not on the same domain as the Jira Software server.

Example: You use user@domain.com as the user identity to crawl http://jira.dev.domain.com.

Notes:

- This parameter is only used when the UseKerberosAuthentication parameter value is true.
- Make sure the user identity exists in both Jira Software and AD.
- When you get the following error:
  
  The Kerberos Authentication failed for user 'userIdentity' with the SPN 'HTTP/ServerName'.

  it means the user identity and/or the SPN are wrong.

Use the following procedure only when you want to modify one or more of the above hidden source parameters.
To modify hidden Jira Software V2 source parameters

1. Refer to "Adding an Explicit Connector Parameter" on page 450 to add one or more Jira V2 hidden source parameters.

2. For a new Jira source, access the Add Source page of the Administration Tool to modify the value of the newly added advanced parameter:
   a. Select Index > Sources and Collections.
   b. Under Collections, select the collection in which you want to add the source.
   c. Under Sources, click Add.
   d. In the Add Source page, edit the newly added advanced parameter value.

3. For an existing Jira Software V2 source, access the Source: ... General page of the Administration Tool to modify the value of the newly added advanced parameter:
   a. Select Index > Sources and Collections.
   b. Under Collections, select the collection containing the source you want to modify.
   c. Under Sources, click the existing Jira Software V2 source in which you want to modify the newly added advanced parameter.
   d. In the Source: ... General page, edit the newly added advanced parameter value.

4. Rebuild your Jira Software V2 source to apply the changes to the parameters.

9.8 Basecamp Connector

CES 7.0.7914+ (October 2015)

The Coveo connector for Basecamp allows Coveo administrators to index and integrate the content of a Basecamp account into the Coveo unified index. The connector indexes all items from a Basecamp account so that in the Coveo search interfaces, a user can easily find Basecamp content.

9.8.1 Features

The Basecamp connector features are:

Content indexing

- Extraction and indexing of the following Basecamp item types:
  - Account
  - Projects
  - Documents
  - Email forwards
  - Messages (standalone discussions)
• To-do lists
• Uploads (stand-alone files)
• To-dos
• Attachments

**Note:** The connector also supports Google Docs attachments.

• Comments

**Note:** Calendars and calendar events are not yet indexed.

**Multithreading**

The connector can run multiple threads, which can improve performances considerably.

**Pause/Resume**

When indexing Basecamp content, the connector can be paused and resumed.

**9.8.2 Limitations**

• The connector does not yet support Basecamp permissions.

**Important:** In the Coveo search interface, a user searching Basecamp content could see content to which he has normally no access in Basecamp. Thus, it is currently highly recommended to only index Basecamp account with public content.

• A full refresh is needed to retrieve the latest items modifications (addition, editon, deletion).

**What's Next?**

Review the steps to deploy the Basecamp connector (see "Basecamp Connector Deployment Overview" on page 830).

**9.8.3 Basecamp Connector Deployment Overview**

The following procedure outlines the steps needed to deploy the Basecamp connector. The steps indicate the order in which you must perform configuration tasks on both the Basecamp and Coveo servers.

**To deploy the Basecamp connector**

1. Validate that your environment meets the requirements (see "Basecamp Connector Requirements" on page 831).

2. (When you want the connector to retrieve your Basecamp content using OAuth 2.0 - recommended method) On the Basecamp server, create an application to authorize the Coveo connector to access your Basecamp content (see "Authorizing the Coveo Connector to Access Your Basecamp Content" on page 831).

3. On the Coveo server, in the Coveo Administration Tool:
a. (When you want to retrieve your Basecamp content using Basic authentication - not recommended)
   Configure a user identity.

   The connector needs to know the credentials of an administrator Basecamp account by creating a CES user identity that you will later associate to your Basecamp source.

b. Create a Basecamp field set to take advantage of the available Basecamp metadata.

   i. It is recommended to start by importing the default Basecamp field set file ([CES_Path]\Bin\Coveo.CES.CustomCrawlers.Basecamp.FieldSet.xml) to create fields for all the metadata available by default from Basecamp items.

   ii. When you created custom metadata for your Basecamp items, add corresponding fields to the field set.

c. Configure and index a Basecamp source.

   The connector must know details to access and index the Basecamp content of your managed users (see "Configuring and Indexing a Basecamp Source" on page 835).

d. If you encounter issues, verify if modifying the default value of hidden source parameters can help resolve the problems (see "Modifying Hidden Basecamp Source Parameters" on page 840).

9.8.4 Basecamp Connector Requirements

Your environment must meet the following requirements to be able to use the Basecamp connector:

- **CES 7.0.7914+ (October 2015)**
- Coveo license for the Basecamp connector
  
  Your Coveo license must include support for the Basecamp connector to be able to use this connector.

- A valid admin Basecamp account

  Using an administrator Basecamp account, you must create a Basecamp app and an OAuth 2.0 protocol to authorize Coveo to access the content of your Basecamp account (see Authorizing the Coveo Connector to Access Your Basecamp Content).

What's Next?

Grant Coveo access to the content of your Basecamp account by creating a Basecamp application (see "Authorizing the Coveo Connector to Access Your Basecamp Content" on page 831).

9.8.5 Authorizing the Coveo Connector to Access Your Basecamp Content

You can grant the Coveo connector access to your Basecamp account content using basic authentication. It is however recommended for security (does not involve passwords) and better performance to perform the complete OAuth 2.0 protocol.

The OAuth 2.0 protocol is a protocol used for granting access to external applications without exposing the user's real credentials. For the connector to be able to connect to the content of your managed users, it must acquire a client ID, a client secret and a refresh token.
To authorize the Coveo connector to access your Basecamp content

**Note:** This topic describes a procedure using Google Chrome and the Advanced Rest Client extension. However, it can be done with other browsers and extensions, such as Firefox and the RESTClient plugin.

1. Create an application using a Basecamp administrator account:
   a. Access Your Applications page.
   b. Log into your Basecamp account with an administrator account.
   c. In the Your Applications page, click Register one now.
   d. In the New application page:
      i. In the About Your application section:
         A. In the first box, enter the Name of your application.
         
         **Example:** Coveo Connector
         
         B. In the second box, enter *Your company’s name*.
         C. In the third box, enter *Your website URL*.
      ii. In the Integration section, select the Basecamp check box.
      iii. In the OAuth 2 authorization section, in the Redirect URI, enter `https://127.0.0.1`.
      iv. Click Register this app.
   e. Back in the Your Applications page:
Your Applications

Register to integrate your application with Basecamp, Highrise, Backpack, and Campfire. Registered apps can authenticate Basecamp IDs and request authorized access to their accounts.

Coveo Connector

Product Access: Basecamp
Client ID: 364cafcdgvy91fc3522b3e0e561bfcb83ff68b
Client Secret: c99a1fcaf4de14fjks39275cf17e3f4f46a30e9
Redirect URI: https://127.0.0.1

Preview authorization dialog

Register Another Application

i. Take note of the following values:

- Client ID
- Client Secret

You need this value when configuring the Basecamp source (see "Configuring and Indexing a Basecamp Source" on page 835).

ii. Click Preview authorization dialog.

f. In the Integrate with [Your App Name] page, click Yes, I'll allow access to receive an authorization code from Basecamp.

g. In your browser address bar, take note of the authorization code returned by the Basecamp API.

**Important:** An authorization code can only be used once before it expires.

**Example:** https://127.0.0.1/?code=[AUTHORIZATION_CODE]

h. Make an API call for an access token and an refresh token:

i. Access the Advanced REST client Google Chrome extension page, and then click the + Free button.

**Note:** You are asked to download Google Chrome if you did not have the browser installed on your computer already.
ii. In the Confirm New App dialog box, click Add.

iii. In the Apps page, open the Advanced REST client plugin.

iv. In the Request tab:

                    Advanced Rest
Client
Request

<table>
<thead>
<tr>
<th>Raw</th>
<th>Form</th>
<th>Headers</th>
</tr>
</thead>
</table>

http://launchpad.37signals.com/authorization/token

- **GET**
- **POST**
- **PUT**
- **PATCH**
- **DELETE**
- **HEAD**
- **OPTIONS**
- **Other**

Raw   Form   Headers

v. Click **Send** to receive an answer.

v. At the bottom of the page, in the Response box, take note of the refresh token value. You need this
value when configuring your Basecamp source (see Configuring and Indexing a Basecamp Source).

What's Next?

Create a Basecamp source ("Configuring and Indexing a Basecamp Source" on page 835).

9.8.6 Configuring and Indexing a Basecamp Source

A source defines a set of configuration parameters for a specific Basecamp account.

To configure and index a Basecamp source

1. On the Coveo server, access the Administration Tool.

2. Select Index > Sources and Collections.

3. In the Collections section:
   a. Select an existing collection in which you want to add the new source.
      OR
   b. Click Add to create a new collection.

4. In the Sources section, click Add.

   The Add Source page that appears is organized in three sections.

5. In the General Settings section of the Add Source page:

   ![General Settings](image)
a. Enter the appropriate value for the following required parameters:

**Name**

Enter a descriptive name of your choice for the connector source.

**Example:** Basecamp

**Source Type**

Select the connector used by this source. In this case, select **Basecamp**.

**Note:** If you do not see **Basecamp**, your environment does not meet the requirements (see "Basecamp Connector Requirements" on page 831).

**Addresses**

This parameter does not apply to this source, but cannot be left empty.

**Example:** https://www.basecamp.com

**Fields**

Select the field set that you created earlier (see Basecamp Connector Deployment Overview).

**Refresh Schedule**

Time interval at which the index is automatically refreshed to keep the index content up-to-date. By default, the **Every day** option instructs CES to refresh the source everyday at 12 AM.

b. Review the value for the following parameters that often do not need to be modified:

**Rating**

Change this value only when you want to globally change the rating associated with all items in this source relative to the rating to other sources.

**Example:** When a source replaces a legacy system, you may want to set this parameter to **High**, so that in the search interface, results from this source appear earlier in the list compared to those from legacy system sources.

**Document Types**

If you defined a custom document type set for this source, select it.

**Active Languages**

If you defined custom active language sets, ensure to select the most appropriate for this source.

6. In the **Specific Connector Parameters & Options** section of the **Add Source** page:
a. Using the following parameters, authorize the Coveo crawler to access the content of your Basecamp account:

**Account ID**

Enter your Basecamp account ID.

*Note: After you login to Basecamp, the account ID can be found in the browser address bar after https://basecamp.com/.*

*Example: https://basecamp.com/3027985/

**Client ID**

(For OAuth 2.0 only) Enter the client identifier to use that you previously obtained (see Authorizing the Coveo Connector to Access Your Basecamp Content).

**Client Secret**

(For OAuth 2.0 only) Enter the client secret to use that you previously obtained (see Authorizing the Coveo Connector to Access Your Basecamp Content).

**Refresh Token**

(For OAuth 2.0 only) Enter the refresh token to use that you previously obtained (see Authorizing the Coveo Connector to Access Your Basecamp Content).

b. In the **Mapping File** box, the path to the default mapping file that defines how the connector handles metadata often does not need to be changed.

c. The following options must be selected for more content in Basecamp to be indexed.
Index Project Drafts

Whether the project drafts should be indexed. By default, archived projects are indexed.

Index Archived Projects

Whether the archived projects should be indexed. By default, archived projects are indexed.

d. (Optional) Click Add Parameter when you want to show and change the value of advanced source parameters (see "Modifying Hidden Basecamp Source Parameters" on page 840).

e. The Option check boxes generally do not need to be changed:

Index Subfolders

This parameter is not taken into account for this connector.

Index the document’s metadata

When selected, CES indexes all the document metadata, even metadata that are not associated with a field. The orphan metadata are added to the body of the document so that they can be searched using free text queries.

When cleared (default), only the values of system and custom fields that have the Free Text Queries attribute selected will be searchable without using a field query.

Example: A document has two metadata:

- LastEditedBy containing the value Hector Smith
- Department containing the value RH

In CES, the custom field CorpDepartment is bound to the metadata Department and its Free Text Queries attribute is selected.

When the Index the document’s metadata option is cleared, searching for RH returns the document because a field is indexing this value. Searching for hector does not return the document because no field is indexing this value.

When the Index the document’s metadata option is selected, searching for hector also returns the document because CES indexed orphan metadata.

Document’s addresses are case-sensitive

Leave the check box cleared. This parameter needs to be checked only in rare cases for systems in which distinct documents may have the same name but different casing.

Generate a cached HTML version of indexed documents

When you select this check box (recommended), at indexing time, CES creates HTML versions of indexed documents. In the search interfaces, users can then more rapidly review the content by clicking the Quick View link rather than opening the original document with the original application. Consider clearing this check box only when you do not want to use Quick View links or to save resources when building the source.
Open results with cached version

Leave this check box cleared (recommended) so that in the search interfaces, the main search result link opens the original document with the original application. Consider selecting this check box only when you do not want users to be able to open the original document but only see the HTML version of the document as a Quick View. In this case, you must also select Generate a cached HTML version of indexed documents.

7. In the Security section of the Add Source page:

![Security Section](image)

**Important:** The connector does not yet support Basecamp permissions. It is thus strongly recommended to only index Basecamp account with public content.

**Note:** A workaround is to manually define permissions on the source (see Permissions).

a. In the Authentication drop-down list, depending on your setup:
   - When you grant the connector access to your Basecamp content using OAuth, select (none).
   - When you want to grant the connector access to your Basecamp content using Basic authentication, select the user identity you previously created (see Basecamp Connector Deployment Overview).

8. Click **Save** to save the source configuration.

9. When your Basecamp content is all public:

**Important:** The connector does not yet support Basecamp permissions. This means that, in the Coveo search interface, a user searching Basecamp content could see content to which he has normally no access in Basecamp.

**Note:** When your Basecamp content is not public, a workaround is to enter the name of user(s) or group(s) you want to allow or deny access to your organization content in the Allowed Users and Deny Users boxes.

a. In the navigation panel on the left, click **Permissions**.

b. In the Permissions page, select Specify the security permissions to index.

c. In the Allowed Users and Denied Users boxes, enter the users and groups that you respectively want to allow or deny to see search results from this source. The default is to allow everyone \$1-1-0\ (Active Directory Group).

d. Click **Apply Changes**.

10. When you are ready to start indexing the Basecamp source, click **Rebuild**.
11. Validate that the source building process is executed without errors:
   - In the navigation panel on the left, click **Status**, and then validate that the indexing proceeds without errors.
   - OR
   - Open the CES Console to monitor the source building activities.

What's Next?

Set an incremental refresh schedule for your source.

Consider modifying some hidden source parameters to try resolving other issues (see "Modifying Hidden Basecamp Source Parameters" on page 840).

9.8.6.1 Modifying Hidden Basecamp Source Parameters

The **Add Source** and **Source: ... General** pages of the Administration Tool present the parameters with which you can configure the connector for most Basecamp setups. More advanced and more rarely used parameters are hidden. You can choose to make one or more of these parameters appear in the **Add Source** and **Source: ... General** pages of the Administration Tool so that you can change their default value. Consider changing values of hidden parameters when you encounter issues.

The following list describes the advanced hidden parameters available with Basecamp sources. The parameter type (integer, string, etc.) appears between parentheses following the parameter name.

**ItemTypesToFold (String)**

Semicolon-separated list of the types of item to fold under their parent. The default value is `Attachment;Comment;Todo`.

**AlwaysFoldOnFirstAncestor (Boolean)**

For items without an indexed parent, whether to allow folding them under their first indexed ancestor. The default value is `False`.

To modify hidden Basecamp source parameters

1. Refer to "Adding an Explicit Connector Parameter" on page 450 to add one or more Basecamp source parameters.

2. For a new Basecamp source, access the **Add Source** page of the Administration Tool to modify the value of the newly added advanced parameter:
   a. Select **Index > Sources and Collections**.
   b. Under **Collections**, select the collection in which you want to add the source.
   c. Under **Sources**, click **Add**.
   d. In the **Add Source** page, edit the newly added advanced parameter value.

3. For an existing Basecamp source, access the **Source: ... General** page of the Administration Tool to modify the value of the newly added advanced parameter:
a. Select Index > Sources and Collections.

b. Under Collections, select the collection containing the source you want to modify.

c. Under Sources, click the existing Basecamp source in which you want to modify the newly added advanced parameter.

d. In the Source: ... General page, edit the newly added advanced parameter value.

4. Rebuild your Basecamp source to apply the changes to the parameters.

9.9 Box Connector

**CES 7.0.7814+ (August 2015)**

The Coveo connector for Box allows Coveo administrators to index and integrate the Box content of their managed users into the Coveo unified index. The connector indexes all items and the attached permissions from all managed users so that in Coveo search interfaces, a user can easily find any but only content to which he has access in Box.

### 9.9.1 Connector Features Summary

<table>
<thead>
<tr>
<th>Features</th>
<th>Supported</th>
<th>Additional information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Box version</td>
<td>☑️ Latest cloud version</td>
<td>Following available Box releases</td>
</tr>
<tr>
<td>Searchable content types</td>
<td>☑️ Enterprises, users, folders, files, and web links</td>
<td></td>
</tr>
<tr>
<td>Incremental refresh</td>
<td>☑️</td>
<td>Full refresh or rebuild needed to:</td>
</tr>
<tr>
<td>Full refresh</td>
<td>☑️</td>
<td>- Remove deleted users in Box</td>
</tr>
<tr>
<td>Rebuild</td>
<td>☑️</td>
<td>- Update the subitems of a renamed folder</td>
</tr>
<tr>
<td>Document-level security</td>
<td>☑️</td>
<td><strong>CES 7.0.8850+ (March 2017)</strong> Support Box permissions.</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Note:</strong> <strong>CES 7.0.8691– (December 2016)</strong> Permissions can only be defined manually on source level [more]**</td>
</tr>
</tbody>
</table>

### 9.9.2 Features

The Box connector features are:

**Content indexing**

Extraction and indexing of the following Box item types:
Mostly supported security model [CES 7.0.8850+ (March 2017)]

The connector mostly supports the Box security model using a security provider to get almost all permissions for each indexed item. This means that, in Coveo search interfaces, a user searching Box content only sees the content to which he has access except items that the user can see using shared links.

**Note:** By default, shared link permissions are ignored, meaning that a document only shared with a link is only visible by its owner in your Coveo search interface. Contact Coveo Support for assistance on how to take shared link permissions into account.

**Incremental refresh**

Supports incremental refresh to periodically query Box for the latest edits, keeping the index content up-to-date.

**Note:** Some changes need a full refresh or a source rebuild to be taken into account (see Limitations).

**Multithreading**

The connector can run multiple threads, which can improve performances considerably (see Configuring and Indexing a Box Source).

**Pause/Resume**

When indexing Box content, the connector can be paused and resumed.

**9.9.3 Limitations**

- Limited incremental capabilities:
  - A full refresh or rebuild is needed to remove deleted users in Box.
  - A full refresh or rebuild is needed to update the subitems of a renamed folder.
  - CES 7.0.8047—(December 2015) When an incremental refresh captures the deletion of a folder in which a collaboration or shared event occur, a warning ("Exception during item expansion") is thrown.
  - CES 7.0.7914—(October 2015) A full refresh or rebuild is needed to retrieve the content (folder and documents) added by a new user in Box.
- Shared link changes are not yet updated.
- CES 7.0.8691—(December 2016) The connector does not support Box permissions.
Important: In the Coveo search interface, a user searching Box content could see content to which he has normally no access in Box. Thus, it is currently highly recommended to only index Box accounts with public content.

- **CES 7.0.8047– (December 2015)** Google docs and Google sheets are not indexed by default. The workaround is to add the Google docs and Google sheet document types manually to the Document Type set used by your Box source (see "Modifying the Document Type Set Used by a Source" on page 481).

- **CES 7.0.7914– (October 2015)** Deleting the folder that represents a specific user in the Index browser is not possible.

### Feature History

<table>
<thead>
<tr>
<th>CES version</th>
<th>Monthly release</th>
<th>Features</th>
</tr>
</thead>
<tbody>
<tr>
<td>7.0.8850</td>
<td>March 2017</td>
<td>Box Enterprise support</td>
</tr>
<tr>
<td>7.0.7814</td>
<td>August 2015</td>
<td>Connector introduction</td>
</tr>
</tbody>
</table>

### What's Next?

Review the steps to deploy the Box connector (see "Box Connector Deployment Overview" on page 843).

### 9.9.4 Box Connector Deployment Overview

The following procedure outlines the steps needed to deploy the Box connector. The steps indicate the order in which you must perform configuration tasks on both the Box and Coveo servers.

#### To deploy the Box connector

1. Validate that your environment meets the requirements (see "Box Connector Requirements" on page 844).

2. On the Box server, authorize the Coveo connector to access the content of your managed users (see "Authorizing the Coveo Connector to Access the Box of Your Managed Users" on page 845).

3. On the Coveo server, in the Coveo Administration Tool:
   a. **CES 7.0.8850+ (March 2017)** Optionally create security providers

      When you want to index Box permissions, you must create two security providers to get Box item permissions and resolve and expand groups.

      In Box, users are identified by their email addresses. Consequently, permissions returned by the Box security provider for each document are email addresses. The Box security provider then requires another security provider to uniquely identify users from their email addresses.

      i. Select or create an Email or an Active Directory security provider that the Box security provider will use to resolve and expand groups. The security provider type to use depends on how users are authenticated when they access the search interface:
When authenticated with their email address, use an Email security provider (see "Configuring an Email Security Provider" on page 85).

When authenticated with an Active Directory account, use an Active Directory security provider (see "Configuring an Active Directory Security Provider" on page 1141).

Notes:

- CES comes with an Active Directory security provider that you can configure to connect to the default domain. When your environment contains more than one domain, you can select an Active Directory security provider that you created for other domains.
- An Active Directory security provider is appropriate only when the User Principal Name (UPN) matches the email address for all users.

Note: You may require to also use a REGEX Transform Member Name security provider in between the two other security providers to map member types. Contact Coveo Support for assistance.

ii. Create a Box security provider that the connector uses to resolve indexed permissions (see "Configuring a Box Security Provider" on page 847).

b. Create a Box field set to take advantage of the available Box metadata.

  i. It is recommended to start by importing the default Box field set file ([CES_Path]\Bin\Coveo.CES.CustomCrawlers.Box.FieldSet.xml) to create fields for all the metadata available by default from Box documents.

  ii. When you created custom metadata for your Box documents, add corresponding fields to the field set.

c. Configure and index a Box source.

   The connector must know details to access and index the Box content of your managed users (see "Configuring and Indexing a Box Source" on page 849).

d. If you encounter issues, verify if modifying the default value of hidden source parameters can help resolve the problems (see "Modifying Hidden Box Source Parameters" on page 854).

9.9.5 Box Connector Requirements

Your environment must meet the following requirements to be able to use the Box connector:

- CES 7.0.7814+ (August 2015)

- Coveo license for the Box connector

  Your Coveo license must include support for the Box connector to be able to use this connector.

- A valid Box Enterprise or Box Business admin, or developer account

  Using a Box Enterprise or Box Business admin, or developer account, you must create a Box app and set up an OAuth 2.0 protocol to authorize Coveo to access the Box content of your managed users (see "Authorizing the Coveo Connector to Access the Box of Your Managed Users" on page 845).
What's Next?

Grant Coveo access to the Box content of your managed users by creating a Box application (see "Authorizing the Coveo Connector to Access the Box of Your Managed Users" on page 845).

9.9.6 Authorizing the Coveo Connector to Access the Box of Your Managed Users

You must perform the server authentication (OAuth 2.0 with JSON Web Token) protocol to authorize the Coveo connector to access the Box content of your managed users.

The OAuth 2.0 protocol is a protocol used for granting access to external applications without exposing the user's real credentials. For the connector to be able to connect to the content of your managed users, it must acquire a client ID and a client secret. You must also create a RSA private-public keypair to sign and authenticate the JSON Web Token (JWT) assertion.

To authorize the Coveo connector to access the Box of your managed users

1. Create an application on a Box account:
   a. Log in to Box with an administrator or developer account.
   b. Enable two-step login verification:
      i. In the menu on the left hand-side of the page, under Account, click Admin Console.
      ii. On the Admin Console page, click the gear icon at the top right, and then click Business Settings.
      iii. In the settings, click the Custom Setup tab.
      iv. In the Custom Setup tab, next to Company Profile, enter a Company Name and a Custom Subdomain, and then, at the bottom of the page, click Save.
   v. Click the Security tab.
   vi. In the Security tab, under Signup and Login, select the Login verification checkbox, and then, at the bottom of the page, click Save.
   vii. Access the Account Settings page:
      A. At the top of the page, click My account.
      B. On the All Files page, in the top right corner, click the drop-down menu with your initials, and then click Account Settings.
   viii. On the Account Settings page, in the Account tab, under Authentication, click Change.
In the Enable Login Verification dialog, enter your Country and Mobile Phone Number, and then click Continue.

You should receive a verification code on your mobile phone shortly.

In the Confirmation Code box, enter the verification code you just received, and then click Continue.

c. Access the My Apps page, in the menu on the left-hand side of the page, by clicking Dev Console.

d. In the My Apps page, click Create New App.

e. In the Create a New Box App page:

i. Select Custom App, and then click Next.

ii. Select OAuth 2.0 with JWT (Server Authentication), and then click Next.

iii. In the Give your app a unique name box, enter a descriptive application name, and then click Create App.

iv. Click View Your App.

f. In the Configuration page:

i. In the OAuth 2.0 Credentials section, take note of the client_id and client_secret values.

   Note: You will need these values when configuring the Box security provider and source (see Configuring a Box Security Provider and Configuring and Indexing a Box Source).

ii. In the Application Scopes section, make sure the Read and write all files and folders stored in Box and Manage groups check boxes are selected. Optionally, if your enterprise uses the App User account feature, also select the Manage users check box.

iii. In the Advanced Features section, make sure Perform Actions as Users is enabled.

iv. In the Add and Manage Public Keys section, click Generate a Public/Private Keypair (see Generating an RSA Keypair).

v. Save the generated config.json file containing your private key, as it will be required later in the Box security provider and source configuration (see Configuring a Box Security Provider and Configuring and Indexing a Box Source).
vi. Note your Public Key ID, as it will be required later in the Box security provider and source configuration (see Configuring a Box Security Provider and Configuring and Indexing a Box Source).

vii. At the top of the page, if you made changes, click Save Changes.

g. Grant access to your enterprise application (see Granting Access in Enterprise Admin Console):

   i. In the menu on the left hand-side of the page, click My Apps.

   ii. In the menu on the left hand-side of the page, under Account, click Admin Console.

   iii. On the Admin Console page, click the gear icon at the top right, and then click Business Settings.

   iv. Click the Apps tab.

   v. In the Apps tab, under Custom Applications, click Authorize New App.

   vi. In the App Authorization dialog that appears, enter your app client_id that you noted previously, and then click Next (see client_id).

   vii. Click Authorize.

What's Next?

- Create a Box security provider ("Configuring a Box Security Provider" on page 847).
- Create a Box source ("Configuring and Indexing a Box Source" on page 849).

9.9.7 Configuring a Box Security Provider

CES 7.0.8850+ (March 2017)

The Coveo Box connector mostly supports the Box security model (see Shared Link Limitation). When you want users searching for Box content in a Coveo search interface to only see the content to which they have access in Box, the connector needs a security provider to be able to index the permissions for each indexed Box item.

**Note:** You can get familiar with how Coveo components deal with permissions on documents both at indexing and query time.

To configure a Box security provider

1. On the Coveo server, access the Administration Tool.

2. Click Configuration, and then Security.

3. In the navigation panel on the left, click Security Providers.

4. In the Security Providers page, click Add to create a new security provider.

5. In the Modify Security Provider page:
a. Configure the following required parameters:

**Name**

Choose a meaningful name to identify the security provider.

*Example: Box Security Provider*

**Security Provider Type**

In the drop-down list, select **Box (x64)**.

**User Identity**

In the drop-down list, select **(none)**.

**Security Provider**

Select the security provider that you selected or created to allow this security provider to resolve and expand the groups (see *Box Connector Deployment Overview*).
Client ID Source

The client identifier to use that you previously obtained (see Authorizing the Coveo Connector to Access the Box of Your Managed Users).

Client Secret Source

The client secret to use that you previously obtained (see Authorizing the Coveo Connector to Access the Box of Your Managed Users).

Enterprise ID Source

The Box Enterprise unique identifier as displayed in your Box Enterprise Admin Console Business Settings page and on the app General settings page.

Public Key ID Source

The public key unique identifier that you previously obtained (see Authorizing the Coveo Connector to Access the Box of Your Managed Users).

Private Key File Source

The full path of the valid PEM private key file that you previously obtained (see Authorizing the Coveo Connector to Access the Box of Your Managed Users).

b. Leave the Allow Complex Identities cleared as it does not apply to this type of security provider.

c. Click Apply Changes.

What's Next?

Create and index a source (see "Configuring and Indexing a Box Source" on page 849).

9.9.8 Configuring and Indexing a Box Source

A source defines a set of configuration parameters for a specific Box account.

To configure and index a Box source

1. On the Coveo server, access the Administration Tool.

2. Select Index > Sources and Collections.

3. In the Collections section:
   a. Select an existing collection in which you want to add the new source.

   OR

   b. Click Add to create a new collection.

4. In the Sources section, click Add.

   The Add Source page that appears is organized in three sections.

5. In the General Settings section of the Add Source page:
a. Enter the appropriate value for the following required parameters:

**Name**

Enter a descriptive name of your choice for the connector source.

**Example:** Box

**Source Type**

Select the connector used by this source. In this case, select **Box**.

**Note:** If you do not see **Box**, your environment does not meet the requirements (see "Box Connector Requirements" on page 844).

**Addresses**

This parameter is not used, but must not be empty. Enter `http://www.box.com`.

**Fields**

Select the field set that you created earlier (see Box Connector Deployment Overview).

**Refresh Schedule**

Time interval at which the index is automatically refreshed to keep the index content up-to-date. By default, the **Every day** option instructs CES to refresh the source everyday at 12 AM. Because the incremental refresh takes care of maintaining the source up-to-date, you can select a longer interval such as **Every Sunday**.

b. Review the value for the following parameters that often do not need to be modified:
Rating

Change this value only when you want to globally change the rating associated with all items in this source relative to the rating to other sources.

**Example:** When a source replaces a legacy system, you may want to set this parameter to **High**, so that in the search interface, results from this source appear earlier in the list compared to those from legacy system sources.

Document Types

If you defined a custom document type set for this source, select it.

Active Languages

If you defined custom active language sets, ensure to select the most appropriate for this source.

6. In the **Specific Connector Parameters & Options** section of the **Add Source** page:

   a. Using the following parameters, authorize the Coveo crawler to access the content of your managed users:

   **Client ID** **Security provider**

   Enter the client identifier to use that you previously obtained (see Authorizing the Coveo Connector to Access the Box of Your Managed Users).
Client Secret

Enter the client secret to use that you previously obtained (see Authorizing the Coveo Connector to Access the Box of Your Managed Users).

Refresh Token

The parameter is not needed when indexing Box Enterprise content.

Enterprise ID **CES 7.0.8850+ (March 2017)**

Enter the enterprise identifier as displayed in your Box Enterprise Settings page. It must be the same ID that you entered when configuring the security provider (see Configuring a Box Security Provider).

Public Key ID **CES 7.0.8850+ (March 2017)**

Enter the public key unique identifier you previously obtained (see Authorizing the Coveo Connector to Access the Box of Your Managed Users). It must be the same ID that you entered when configuring the security provider (see Configuring a Box Security Provider).

Private Key File **CES 7.0.8850+ (March 2017)**

Enter the full path of the valid PEM private key file you previously obtained (see Authorizing the Coveo Connector to Access the Box of Your Managed Users). It must be the same file path that you entered when configuring the security provider (see Configuring a Box Security Provider).

b. The default value for the following parameter generally does not need to be changed:

**Number of refresh threads**

Determines the number of files that the connector can refresh simultaneously. The default and recommended value is 8.

c. The following option must be selected for your managed users content to be indexed.

**Index Managed Users' Content**

*Note: CES 7.0.9093– (September 2017) The parameter was labeled Index All Managed Users.*

Whether the content of all your managed users should be indexed. When the option is cleared, only your content is indexed.

d. **CES 7.0.9167+ (December 2017)** When you want Box users to be indexed as separate documents, select the following option:

**Index Users**

e. Select additional content to be indexed using the following option:

**Index Custom File Metadata**

Whether the custom metadata specified in the Global Properties should be indexed.

f. (Optional) Click Add Parameter when you want to show and change the value of advanced source parameters (see "Modifying Hidden Box Source Parameters" on page 854).

g. The **Option** check boxes generally do not need to be changed:
Index Subfolders

This parameter is not taken into account for this connector.

Index the document's metadata

When selected, CES indexes all the document metadata, even metadata that are not associated with a field. The orphan metadata are added to the body of the document so that they can be searched using free text queries.

When cleared (default), only the values of system and custom fields that have the **Free Text Queries** attribute selected will be searchable without using a field query.

**Example:** A document has two metadata:

- LastEditedBy containing the value Hector Smith
- Department containing the value RH

In CES, the custom field **CorpDepartment** is bound to the metadata **Department** and its **Free Text Queries** attribute is selected.

When the **Index the document's metadata** option is cleared, searching for RH returns the document because a field is indexing this value. Searching for hector does not return the document because no field is indexing this value.

When the **Index the document's metadata** option is selected, searching for hector also returns the document because CES indexed orphan metadata.

Document's addresses are case-sensitive

Ensure that this option is selected because Dropbox team member IDs are case sensitive.

Generate a cached HTML version of indexed documents

When you select this check box (recommended), at indexing time, CES creates HTML versions of indexed documents. In the search interfaces, users can then more rapidly review the content by clicking the **Quick View** link rather than opening the original document with the original application. Consider clearing this check box only when you do not want to use **Quick View** links or to save resources when building the source.

Open results with cached version

Leave this check box cleared (recommended) so that in the search interfaces, the main search result link opens the original document with the original application. Consider selecting this check box only when you do not want users to be able to open the original document but only see the HTML version of the document as a **Quick View**. In this case, you must also select **Generate a cached HTML version of indexed documents**.

7. When you chose to index Box permissions, in the **Security** section, in the **Security Provider** drop-down list, select the Box security provider that you created for this source (see “Configuring a Box Security Provider” on page 847).
8. Click **Save** to save the source configuration.

9. When your Box content is all public or when you use CES 7.0.8691– (December 2016):
   a. In the navigation panel on the left, click **Permissions**.
   b. In the **Permissions** page, select **Specify the security permissions** to index.
   c. In the **Allowed Users** and **Denied Users** boxes, enter the users and groups that you respectively want to allow or deny to see search results from this source. The default is to allow everyone `\$-1-1-0\` (Active Directory Group).
   d. Click **Apply Changes**.

10. When you are ready to start indexing the Box source, click **Rebuild**.

11. Validate that the source building process is executed without errors:
    - In the navigation panel on the left, click **Status**, and then validate that the indexing proceeds without errors.
    - OR
    - Open the CES Console to monitor the source building activities.

What's Next?

- Set an incremental refresh schedule for your source.

- Consider modifying some hidden source parameters to try resolving other issues (see "Modifying Hidden Box Source Parameters" on page 854).

9.9.8.1 Modifying Hidden Box Source Parameters

The **Add Source** and **Source: ... General** pages of the Administration Tool present the parameters with which you can configure the connector for most Box setups. More advanced and more rarely used parameters are hidden. You can choose to make one or more of these parameters appear in the **Add Source** and **Source: ... General** pages.
pages of the Administration Tool so that you can change their default value. Consider changing values of hidden parameters when you encounter issues.

The following list describes the advanced hidden parameters available with Box sources. The parameter type (integer, string, etc.) appears between parentheses following the parameter name.

**RetrieveGlobalFileMetadata (Integer)**

Whether to retrieve the global metadata (properties) of files. The default value is *false*.

**RetrieveFileCommentsMetadata (Integer)**

Whether to retrieve the file comments as a metadata. The default value is *false*.

**IgnoreSharedLinkPermissions (Boolean)**

Whether to ignore Shared Link permissions. The default value is *true*.

**Important:** Setting this parameter to *false* can potentially expose sensitive information as all documents that were shared using a Share Link will be considered public.

**IgnoreSharedLinkPasswordProtection (Integer)**

Whether to ignore Shared Link password protection when **IgnoreSharedLinkPermissions** is *false*. The default value is *false*.

To modify hidden Box source parameters

1. Refer to "Adding an Explicit Connector Parameter" on page 450 to add one or more Box source parameters.

2. For a new Box source, access the **Add Source** page of the Administration Tool to modify the value of the newly added advanced parameter:
   a. Select **Index > Sources and Collections**.
   b. Under **Collections**, select the collection in which you want to add the source.
   c. Under **Sources**, click **Add**.
   d. In the **Add Source** page, edit the newly added advanced parameter value.

3. For an existing Box source, access the **Source: ... General** page of the Administration Tool to modify the value of the newly added advanced parameter:
   a. Select **Index > Sources and Collections**.
   b. Under **Collections**, select the collection containing the source you want to modify.
   c. Under **Sources**, click the existing Box source in which you want to modify the newly added advanced parameter.
   d. In the **Source: ... General** page, edit the newly added advanced parameter value.

4. Rebuild your Box source to apply the changes to the parameters.
9.10 Database Connector

The Coveo connector for databases allows to index database content directly through an ODBC connection and SQL queries.

9.10.1 Supported databases

The Database connector can index the following databases:

- Microsoft SQL Server
- Any database that has an OLE DB provider
- Any database that has an ODBC provider, including Oracle and DB2

9.10.2 Connector Features

The features of the Database connector are:

**Database indexing**

Fully customizable database indexing, either by specifying SQL queries or item types (table names).

**Incremental Refresh**

The connector uses one column to track changes and only fetch the updated rows (see "Enabling Incremental Refresh on a Database Source" on page 879).

**Note:** A source full refresh or rebuild is required to take deleted items into account.

**Authentication and identity replacement**

The connector supports standard authentication to databases (username and password), however you can hide the password and username by introducing the @pwd and @uid tokens. By doing so, it is not possible to see passwords in clear text, even if one has access to CES Administration (see "Replacing the Identity in Database Connection Strings" on page 878).

**Complement information retrieval using subqueries**

The connector indexes documents through a query against a database. Subqueries can run on every document to complete the information with more complex queries (see "Complement Information Retrieval with Subqueries for the Database Connector" on page 882).

**Support running in 32-bit**

On a 64-bit platform, the 64-bit version of the connector can use ODBC providers in both 32-bit and 64-bit.

**Query-based security provider**

You can expand external groups and users using a security provider when the database contains information allowing groups to be expanded to external users and/or external users to be mapped to Active Directory users (see "Enabling a Query-Based Security Provider for the Database Connector" on page 881).
Paged query execution

The connector mapping file can be configured to support executing queries in smaller subsets of data, instead of one big result; therefore the time required to execute a query can considerably be reduced (see "Enabling Paged Query Execution for the Database Connector" on page 866).

Multithreading

The connector can run multiple threads, which can improve performances considerably (see "Enabling Multithreading for the Database Connector" on page 877).

Field mapping

Fully customizable field mapping, from your database fields to CES custom and system fields.

Pause/Resume

You have the possibility to pause and resume while indexing a database (see "Enabling Pause/Resume on a Database Source" on page 879).

Indexing custom permissions

The connector can index custom permissions predefined for each document indexed.

Redirecting hyperlinks

Capability to redirect the hyperlink of a document to an existing Web interface or its Quick View of a respective HTML cached version.

What's Next?

Get familiar with the steps to deploy the Database connector (see "Database Connector Deployment Overview" on page 857).

9.10.3 Database Connector Deployment Overview

The following procedure outlines the steps required to deploy the Database connector. The steps indicate the order in which to perform required and optional configuration tasks.

1. Validate that your environment meets the requirements (see "Database Connector Requirements" on page 859).

2. In your DBMS, select or create a crawling account (user) that will be used by the CES connector. The CES connector requires a Full Read DBMS account that is able to read all tables referred to in the mapping file. Refer to the documentation specific to your DBMS.

   A best practice is to create a fixed password account that is used exclusively by the Coveo connector.

3. Create a configuration file

   You must create a configuration file that instructs the connector how to crawl the database for a given source. You can either create a configuration file from scratch or customize the provided sample file (see "Indexing a Database Using a Configuration File" on page 859).

4. On the Coveo server, in the Coveo Administration Tool:
a. Optionally create a CES database user identity

When you want to hide the account credentials in the database connection string, you can configure a user identity using the credentials of the crawling account that you selected or created in Step 2 (see "Adding a User Identity" on page 420) and use tokens in the database connection string (see "Replacing the Identity in Database Connection Strings" on page 878).

b. Optionally create security providers

When you want to index database permissions, you must create two security providers to get database group definition permissions (if any) and resolve and expand groups.

i. Start by selecting or creating a security provider that the Database security provider will use to resolve and expand groups. The security provider type to use depends on how users are authenticated when they access your Coveo search interface:

   **Note:** CES 7.0.7.0.8850+ (March 2017) You may require to also use a REGEX Transform Member Name security provider in between the two following security providers to map member types (see "Configuring a REGEX Transformation Security Provider" on page 67). Contact Coveo Support for assistance.

   - CES 7.0.7.0.8850+ (March 2017) When authenticated with their email address, use an Email security provider (see "Configuring an Email Security Provider" on page 65).
   - When authenticated with an Active Directory account, use an Active Directory security provider (see "Configuring an Active Directory Security Provider" on page 1141).

   **Notes:**
   - CES comes with an Active Directory security provider that you can configure to connect to the default domain. When your environment contains more than one domain, you can select an Active Directory security provider that you created for other domains.
   - An Active Directory security provider is appropriate only when the User Principal Name (UPN) matches the email address for all users.

ii. Then create a Database security provider that the connector uses to resolve indexed permissions (see "Configuring a Database Security Provider" on page 867).

c. Configure and index the Database source

   The connector must know details about the database to index its content (see "Configuring and Indexing a Database Source" on page 869).

d. Optionally, use paged query execution

   If you encounter time out or performance issues, consider using paged queries to try resolving the issues (see "Enabling Paged Query Execution for the Database Connector" on page 866).

e. Optionally, customize the configuration file to fine-tune indexed content
Once your Database source is up and running, you can customize the configuration file of the connector to fine-tune the indexed content or index other tables in your DBMS (see "Example of a Configuration File for the Database Connector" on page 860 and "Additional XML Attributes" on page 865).

9.10.4 Database Connector Requirements

Your environment must meet the following requirements in order to use the Database connector:

- Coveo license for the Database connector
  Your Coveo license must include support for the Database connector to be able to use this connector.
- A database with ODBC or OLE DB provider
- Open ports

When the access to communication ports between the Coveo Master server and the database server(s) is restricted, the appropriate database ports must be opened in the network infrastructure such as in firewalls to allow the Coveo connector to access the content (see Common Database Server Port Numbers or Configure the Windows Firewall to Allow SQL Server Access or Ports That Must Be Open to Make an ODBC or Data Transfer Connection through a Firewall).

9.10.5 Indexing a Database Using a Configuration File

You can use a configuration file to index data from a database. This file instructs the connector on the way to retrieve and copy the data from the record fields to the Coveo system and custom fields.

Considering that the required URI field is used as the underlying link of a search result, it is important to determine where a user is redirected when a result is opened.

- Best case scenario, a Web interface displays the results of the search, making it easy to recreate the address of a record page with fields from your database.
- Worst case scenario, the users are not redirected when they click on a search result.

**Note:** If the Open results with cached version option is selected, the document automatically opens in the Quick View (see "Configuring and Indexing a Database Source" on page 869).

To setup a configuration file

1. Create an XML-formatted configuration file and save it on the Coveo server. It is possible to create one from scratch or from the provided sample (see "Example of a Configuration File for the Database Connector" on page 860).

   **Note:** It is recommended to save it in the CES configuration folder ([Index_Path]\Config, by default C:\CES7\Config).

2. Create a database source and specify the path of the configuration file using the Configuration File Path source parameter (see "Configuring and Indexing a Database Source" on page 869).
9.10.5.1 Example of a Configuration File for the Database Connector

You can use the following configuration file with the Database connector to index data from the sample Northwind database that can be used with Microsoft Access and Microsoft SQL Server.

Notes:

- The following configuration file example will work with the Northwind database available from Microsoft Access 2013. When using other versions, validate that schema of your Northwind database matches with the parameter names in the following configuration file example.

- In the following example, you must replace [PARAMETER] by @LastRefresh in an SqlClient scenario or by ? otherwise.

- A Database source can regularly run incremental refreshes to re-index only the latest changed information from the database when you configure incremental refresh (see "Enabling Incremental Refresh on a Database Source" on page 879).

```xml
<?xml version="1.0" encoding="utf-8" ?>
<ODBC>
  <CommonMapping excludedItems="Customers">
    <AllowedUsers>
      <AllowedUser type="Windows" allowed="true">
        <Name>everyone</Name>
        <Server></Server>
      </AllowedUser>
    </AllowedUsers>
  </CommonMapping>
  <Mapping type="Orders">
    <Accessor type="query">
      SELECT Shippers.Company AS ShipperName,
      Orders.[Order ID] AS ID,
      Orders.[Customer ID],
      Orders.[Order Date],
      Orders.[Shipped Date],
      Customers.Company,
      Employees.[Last Name],
      Employees.[First Name],
      Products.[Product Name],
      Products.[List Price]
      FROM Orders, [Order Details], Shippers, Customers, Employees, Products
      WHERE Orders.[Shipper ID] = Shippers.ID AND
      Orders.[Customer ID] = Customers.ID AND
      Orders.[Employee ID] = Employees.ID AND
      [Order Details].[Order ID] = Orders.[Order ID] AND
      [Order Details].[Product ID] = Products.ID AND
      Orders.[Order Date] >= [PARAMETER]
    </Accessor>
    <Fields>
      <ClickableUri>http://www.coveo.com</ClickableUri>
      <FileName>%(ID).txt</FileName>
      <Title>Order ID: %(ID): %(Product Name)</Title>
      <ModifiedDate>%(OrderDate)</ModifiedDate>
      <Body>
        Customer: %(Company)
        OrderDate: %(Order Date)
        ShippedDate: %(Shipped Date)
        Shipped via: %(ShipperName)
        %(Product Name), $%(List Price)
      </Body>
    </CustomFields>
    <CustomField name="Type">Order</CustomField>
  </Mapping>
</ODBC>
```
The following list presents the different attributes found in the sample configuration file:

<CommonMapping>

You can specify multiple settings common for all or several of the mappings in the configuration file. Unless specified otherwise, <CustomFields> and <AllowedUsers> nodes used for all tables can be added (see "<Mappings> on page 862). The excludedItems attribute lists all the objects from the ItemType source parameter that does not use the settings specified in CommonMapping. The following represents the entire CommonMapping nodes where the table Customers is excluded.

Refer to the following example:

<CommonMapping excludedItems="Customers">
  <Fields>
    <CustomField name="ID">%[ID]</CustomField>
  </Fields>
  <AllowedUsers>
    <AllowedUser type="Windows" allowed="true">
      <Name>everyone</Name>
    </AllowedUser>
  </AllowedUsers>
</CommonMapping>
<Mapping>

Defines how the connector retrieves data from the tables, how the indexed data is stored, and who has access to it. It has an attribute called type. It is important to add the name of the table used for mapping. The mapping for the table Orders is displayed and two tables are indexed, however one contains the most complex configuration.

Refer to the following example:

**Note:** All node values can be defined using the following syntax: `%[odbcField]`. When the indexing process starts, this value is replaced by the actual value from the Database source. For example, in `<FileName>%[CustomerID].txt</FileName>`, the term `%[CustomerID]` is dynamic and replaced by the source value; however, `.txt` is static.

<Accessor>

The `<Accessor>` node contains the query string used to extract the data from the table. This node is mandatory in order to have a valid mapping. It defines the method used to access the specified table. There is an attribute called type that can either be equal to object or query. In the example above, the query type is used, meaning that the information stored in the database is accessed using a SQL query and can be stored in multiple tables and views.

Refer to the following example where you must replace `[PARAMETER]` by `@LastRefresh` in an SqlClient scenario or by `?` otherwise:

```sql
SELECT Shippers.Company AS ShipperName,
    Orders.[Order ID] AS ID,
    Orders.[Customer ID],
    Orders.[Order Date],
    Orders.[Shipped Date],
    Customers.Company,
    Employees.[Last Name],
    Employees.[First Name],
    Products.[Product Name],
    Products.[List Price]
FROM Orders, [Order Details], Shippers, Customers, Employees, Products
WHERE Orders.[Shipper ID] = Shippers.ID AND
    Orders.[Customer ID] = Customers.ID AND
    Orders.[Employee ID] = Employees.ID AND
    [Order Details].[Order ID] = Orders.[Order ID] AND
    [Order Details].[Product ID] = Products.ID AND
    Orders.[Order Date] >= [PARAMETER]
```

**Note:** You can use the paged query execution feature to return results in small batch number and decrease the likelihood of execution timeout (see "Enabling Paged Query Execution for the Database Connector" on page 866).

<Fields>

Collection of fields to be mapped when a document is indexed.

(Uri>

Address to which the user is redirected when clicking on the title of a search result. It is also used by the index to identify documents.
Refer to the following example:


**Note:** Even though the indexed database records do not have an actual Web address where they can be viewed by users, you must provide one. It is possible to generate an URI based on any dummy address as long as it is unique. You can create one formed with a primary key provided from your database.

<ClickableUri>

URI opened when trying to open documents from the user interface of CES.

Refer to the following example:

<ClickableUri>http://www.coveo.com</ClickableUri>

<FileName>

Name of the file indexed. The extension of the filename is used to select the appropriate converter.

Refer to the following example:

<FileName>%[ID].txt</FileName>

<Title>

Name displayed on the search result page representing the title of the document indexed.

Refer to the following example:

<Title>Order ID: %[ID]: %[Product Name]</Title>

**Note:** %[ID] and %[Product Name] are used to give each entry its own name based on the ID and product name fields in the Orders table.

<Body>

Body of the document indexed. It can be a mix of static and dynamic content taken from the table.

Refer to the following example:

<Body>

Customer: %[Company]
OrderDate: %[Order Date]<br/>
ShippedDate: %[Shipped Date]<br/>
Shipped via: %[ShipperName]<br/>
%[Product Name], %[List Price]
</Body>

<Body>OrderDate: %[Order Date] \nRequiredDate: %[Required Date] \nShippedDate: %[ShippedDate] \\
Shipped via: %[ShipperName] 
</Body>

The fields (%[field_name]) are all dynamic content types that change with each entry taken from the table.

**Note:** You cannot use both Body and BinaryBody nodes at the same time.
<CustomFields>

Mapping of ODBC fields to CES custom fields. It is made of a collection of <CustomField> nodes.

<CustomField>

Each <CustomField> node represents a custom field in CES and the data contained therein. In the example above, several <CustomField> nodes like the following are displayed:

<CustomField name="OrderDate">%[Order Date]</CustomField>

The name attribute is mandatory and represents the name of the CES custom field to bind data to. The value of this node should use the mapping syntax. The %[Order Date] expression instructs the connector to copy the information from the OrderDate database field to the OrderDate custom field in CES.

<AllowedUsers>

Mapping of ODBC fields to CES security. The connector does not index the permissions of the database automatically, therefore this field can be used to protect the data taken from the database.

**Note:** If you do not insert this section, everybody will have access to all the documents indexed.

<AllowedUser>

Rights given to users or groups regarding indexed documents. In the following example, there are two mandatory attributes:

Refer to the following example:

<AllowedUser type="CustomGroup" allowed="true">

- **Type:** It specifies the type of user to which rights are given (Windows, CustomGroup or CustomUser).
- **Allowed:** It can be set to true or false.

**Note:** You can define multiple allowed users within a single AllowedUser node by separating them by a semicolon (;).

{Name>

Name of a user or group to which you want to grant permissions. The FirstName and LastName values are used and stored in the table. This type of setup is useful only if these fields correspond to users that have access to the database.

Refer to the following example:

{Name> %[First Name] %[Last Name] </Name>

You should have one or more tables listing the users as well as their respective permissions. Also, provide the name of a Windows group that contains all the users that should have access. Otherwise, this field can be set to Everyone, meaning everyone has access to the information taken from the table.
<Server>

Domain name for the current group or user. In the above example, no server name is specified. However, in an everyday context, it needs to be set to a specific value.

9.10.5.2 Additional XML Attributes

This section presents additional XML attributes necessary to index data from a database. Basically, a single mandatory section must be included in a configuration file: the Mapping node, which must be placed under a parent ODBC node.

The following displays this basic structure:

```xml
<?xml version="1.0" encoding="utf-8" ?>
<ODBC>
  <CommonMapping>
    </CommonMapping>
  <Mapping>
    </Mapping>
</ODBC>
```

**Note:** The CommonMapping node is optional.

<CommonFields>

As in the Mapping section, it is a Fields node that is added to all mappings except the ones specified in the ExcludedItems list. This list is made of comma (,) separated values.

Refer to the following example:

```xml
<CommonFields excludedItems="ItemType">
  </CommonFields>
```

</Mapping type=" ">

Each Mapping node must have a type attribute. This attribute represents the name of this mapping and is the value used to reference a mapping.

<BinaryBody>

This node is used to map a BLOB field from the database to the body of the document. Exceptionally, the value specified for this node must not use the standard syntax %[odbcField]. Instead, use the syntax odbcField. Once the mapping is resolved, an appropriate converter is called depending on the type of file inside the BLOB field of the database.

**Note:** You cannot use both BinaryBody and Body nodes at the same time.

<PrintableUri>

URI displayed in the user interface of CES.

<ContentType>

Type of data in the body of the document. Either this node or <FileName> must be specified, as it is used to find the appropriate converter. If you are not sure of the type of data being indexed, use the binarydata value and CES will find the right converter for your document data. The mapping syntax should be used to define the
mapping of this field.

**Note:** For database records without an actual filename, do not specify the `<FileName>` node; however, do specify the `<ContentType>text/html</ContentType>` node.

**<ModifiedDate>**

Last modification date on a document. The value of this field must be a date, and the mapping syntax should be used to define the mapping of this field.

9.10.5.3 Enabling Paged Query Execution for the Database Connector

The amount of data to retrieve and the time it takes to execute a query can sometimes be a lengthy process. This is why the Database connector can execute queries in smaller subsets of data - called page result - allowing the retrieval of, for example, 5,000 rows per call. By doing so, timeouts can easily be avoided.

The paged query execution takes advantage of a feature found on most DBMS, which offers the possibility to retrieve the subset of query results by specifying the range of rows to crawl.

**Note:** For the initial release of the paged query execution feature, SQL Server and Oracle are the officially supported DBMS supporting this mode of operation.

To take advantage of the paged query execution feature, you must properly configure your mapping file. You have to provide a query that takes advantage of the paging feature and supply two tokens (@startRow and @endRow) that will dynamically be replaced at run time by the connector with the actual range of data to retrieve. When these tokens are detected, the connector automatically enables paging execution.

Refer to the following for an excerpt of a mapping file with a query configured to run in paged mode against SQL Server:

```sql
SELECT * FROM (  
    SELECT MESSAGE.MID,  
    MESSAGE.SENDER,  
    MESSAGE.DATE,  
    MESSAGE.MESSAGE_ID,  
    MESSAGE.SUBJECT,  
    MESSAGE.BODY,  
    MESSAGE.FOLDER,  
    ROW_NUMBER() OVER (Order By MESSAGE.MID) as LINE  
FROM MESSAGE  
WHERE MESSAGE.DATE_ LIKE '2001-04-07%' ) RESULTS  
WHERE RESULTS.LINE between @startRow and @endRow
```

All queries in a configuration file are independent. You can decide to use the paged query execution feature or not.

**Example:** A query can be written as a paged query, while its associated subqueries can be written without this feature.

**Hidden parameter for page size (Integer)**

By default, the connector is configured to query the database 5,000 records at a time when the paged query execution feature is enabled. However, this value can be overridden by configuring the `QueryPageSize` hidden parameter in the source configuration. The value should be positive and different from 0.
To configure the QueryPageSize hidden parameter

1. On the Coveo server, access the Administration Tool.
2. Add the QueryPageSize hidden parameter to the database connector for all database sources by specifying an Integer type and 5000 for the default value (see "Adding an Explicit Connector Parameter" on page 450).
3. Select the Index tab, and then select the Sources and Collections menu.
4. For each database source for which you want to change the default value for the QueryPageSize parameter:
   a. Under Collections, select the collection containing the database source.
   b. Under Sources, select the desired database source.
   c. In the navigation panel on the left, select General.
   d. In the Query Page Size box that now appears in the page, enter the desired page size value for this database source. The value should be positive and different from 0.
   e. Click Apply Changes.

9.10.6 CES Configuration for the Database Connector

9.10.6.1 Configuring a Database Security Provider

When your database contains permission information and user group definitions, you can use a security provider to expand the groups and index the permissions stored in the database. Otherwise, you do not need a security provider.

Note: You can get familiar with how Coveo components deal with permissions on documents both at indexing and query time.

To create or modify a database security provider

1. On the Coveo server, access the Administration Tool.
3. In the navigation panel on the left, select Security Providers.
4. In the Security Providers page:
   - Click Add to create a new security provider.
     OR
   - Click an existing security provider to modify it.
5. In the Modify Security Provider page:
a. In the Name box, enter a name to identify this security provider.

b. In the Security Provider Type drop-down list:
   i. On a 32-bit server, select **Database (x86)**.
   ii. On a 64-bit server, select **Database (x64)**, or when the database driver used is a 32-bit process, select **Database (x86)**.

c. In the User Identity section, select a user identity only when you want to hide the account credentials in the Database Connection String:
   i. In the drop-down list, select the user identity that you selected or created to crawl your databases.
   ii. When this is not already done, click **Add**, **Edit**, or **Manage user identities** respectively to create, modify, or manage user identities.

d. In the Security Provider drop-down list:

   **Note:** CES 7.0.8691– (December 2016) The parameter was labeled **Active Directory Security Provider**.
i. Select the security provider that you selected or created to allow this security provider to resolve and expand the groups (see Database Connector Deployment Overview).

ii. When an appropriate security provider is missing, click Add, Edit, or Manage security providers respectively to create, modify, or manage security providers.

e. In the Database Connection String box, enter the connection string used to connect to the database. The connection string syntax differs from one database type to another. Refer to the appropriate documentation for the format of the connection string specific to your database (see www.connectionstrings.com).

   **Note:** When you assign a user identity to the security provider, you can hide the password and the user ID by replacing them with tokens in the connection string (see "Replacing the Identity in Database Connection Strings" on page 878).

f. In the Drive Type box, enter the type of the driver used to connect to the database:
   - Enter Odbc for Open Database Connectivity.
   - Enter OleDb for Object Linking and Embedding, Database.
   - Enter SqlClient for an SQL client.

g. In the Query Page Size box, enter the desired page size value for an ODBC query when executing in paged mode. The value should be positive and different from 0. The default value is 5000.

h. In the Query Timeout Time box, enter the maximum time (in milliseconds) allowed to perform a query on the database. The default value is 60000 ms (60 seconds).

i. In the Parameters section, in rare cases, the Coveo Support could instruct you to click Add Parameters to specify other security provider parameter names and values that could help to troubleshoot security provider issues.

j. Leave the Allow Complex Identities option cleared as it does not apply to this type of security provider.

k. Click Save or Apply Changes, depending whether you are creating or modifying a security provider.

**What's Next?**

Create an index a source ("Configuring and Indexing a Database Source" on page 869).

### 9.10.6.2 Configuring and Indexing a Database Source

A source defines a set of configuration parameters for the databases indexed, including all the information required to access and authenticate.

To configure and index a database source

1. On the Coveo server, access the Administration Tool.
2. Select Index > Sources and Collections.
3. In the Collections section:
a. Select an existing collection in which to add the new source.

OR

b. Click Add to create a new collection.

4. In the Sources section, click Add to create a new database source.

The Add Source page that appears is organized in three sections.

5. In the General Settings section of the Add Source page:

a. Enter the appropriate value for the following required parameters:

Name

Enter a descriptive name of your choice for the connector source.

Example: Employee database

Source Type

Select the connector used by this source. In this case, select Database.

Note: If you do not see Database, your environment does not meet the requirements (see “Database Connector Requirements” on page 859).

Addresses

Enter the connection string used to connect to the database. The connection string syntax differs from
one database type to another. Refer to the appropriate documentation for the format of the connection string specific to your database (see www.ConnectionStrings.com).

The same connection string can be used for different sources. However, there can only be one connection string per source.

**Example:** Data Source=dbServer.company.com;Initial Catalog=employees;UserId=companyUser;Password=MyPassword

You can hide the password and the user ID in the connection string (see "Replacing the Identity in Database Connection Strings" on page 878).

**Note:** When the ODBC connection string includes SSPI security, CES uses the CES Service logon account to connect to the database. Ensure that the CES service of your Coveo instance uses a domain account that can crawl the database, not a local system account.

**Refresh Schedule**

Time interval at which the source is automatically refreshed to keep the index content up-to-date. By default, the recommended *Every day* option instructs CES to refresh the source everyday at 12 AM.

**Note:** You can create new or modify existing source refresh schedules.

6. In the **Specific Connector Parameters & Options** section of the **Add Source** page:
a. Enter the appropriate value for the following required parameters:

**Items to crawl**

Enter a comma-separated (,) list of table or view object names to crawl as they are defined in the configuration file. You can use this parameter to easily crawl a subset of objects defined in the configuration file rather than commenting out objects in the configuration file.

**Configuration File Path**

Enter the full path to the configuration file that you created to instruct the connector what to index (see "Indexing a Database Using a Configuration File" on page 859).

**Example:** C:\CES7\Config\odbc_config.xml

b. Review the value for the following parameters that often do not need to be modified:

**Number of Refresh Threads**

Determines the number of simultaneous downloads handled by the connector.

**Command Timeout**

Maximum time allowed to perform a query on the database. The default value is 60 seconds. Once elapsed, the query times out.

**Note:** You can use the paged query execution feature to decrease the execution time (see "Enabling Paged Query Execution for the Database Connector" on page 866).

**Use 32 bits driver**

On a 64-bit server, select this check box when you use a 32-bit driver to connect to the database.
**Note:** Selecting the **Use 32 bits driver** option may resolve issues causing the **Arithmetic operation resulted in an overflow** error that appears to be linked to the 64-bit driver inability to convert a database field. However, updating to the ODBC driver 5.3+ also can resolve the problem.

**Driver Type**

- In the drop-down box, select the software driver that provides access to your database:
  - Select **Odbc** when using Open Database Connectivity.
  - Select **OleDb** when using Object Linking and Embedding, Database.
  - Select **SqlClient** when using an SQL client.

**Index Subfolders**

This parameter does not apply to a database source.

**Index the document’s metadata**

- When selected, CES indexes all the document metadata, even metadata that are not associated with a field. The orphan metadata are added to the body of the document so that they can be searched using free text queries.

- When cleared (default), only the values of system and custom fields that have the **Free Text Queries** attribute selected will be searchable without using a field query.

**Example:** A document has two metadata:

- LastEditedBy containing the value Hector Smith
- Department containing the value RH

In CES, the custom field **CorpDepartment** is bound to the metadata **Department** and its **Free Text Queries** attribute is selected.

When the **Index the document’s metadata** option is cleared, searching for **RH** returns the document because a field is indexing this value. Searching for **hector** does not return the document because no field is indexing this value.

When the **Index the document’s metadata** option is selected, searching for **hector** also returns the document because CES indexed orphan metadata.

**Document’s addresses are case-sensitive**

- Leave this check box cleared. This parameter needs to be checked only in rare cases for systems in which distinct documents may have the same name but different casing.

**Generate a cached HTML version of indexed documents**

- Keep this check box selected. When indexing, CES creates HTML versions of indexed documents. In the search interfaces, users can review the content more rapidly by clicking the **Quick View** link.

- Consider clearing this check box only when you do not want to use **Quick View** links or save resources.
when building the source.

**Open results with cached version**

Select this check box to view the cached HTML version of the database content when the end-user clicks the main search result link. In this case, you must also select **Generate a cached HTML version of indexed documents**.

Clear this check box only when you defined a clickable URI in the configuration file to open the database content in a specific application. Do not want users to be able to open the original document but only see the HTML version of the document as a Quick View.

7. In the **Security** section of the **Add Source** page:

   ![Security section of Add Source page]

   a. In the **Security Provider** drop-down list, when you chose to use a security provider, select the security provider that you created for this source (see "Configuring a Database Security Provider" on page 867).

   b. In the **Authentication** drop-down list, when you chose to hide the database account credentials in the database connection string, select the user identity that you created for this source (see "Adding a User Identity" on page 420).

   c. Click **Save and Start** to save the source configuration and start indexing this source.

8. Validate that the source building process is executed without errors:

   - In the navigation panel on the left, click **Status**, and then validate that the indexing proceeds without errors.

   OR

   - Open the CES Console to monitor the source building activities.

9.10.6.3 Creating a View in a Database

You can exploit the principle of embedded views (queries) in a database, therefore not having to rewrite long, complex queries in a configuration file.

**Note:** If you have to use a configuration file, your query expression can be used to filter out objects you do not want from an existing View.
To create a view in a database

1. Log on to your database with a database editor/client.

   **Note:** Make sure you have the appropriate read/write rights or administrator privileges for the database.

2. On the command line of the client, create your view. If you are using an access-like database editor, create a view only using the `SELECT` and `FROM` parts of the queries provided below.

   - **CES_Orders**
   
   Security permissions for documents should be defined using one of the methods explained in "Indexing a Database Using a View" on page 876.

   ```sql
   CREATE view "CES_Orders" AS
   SELECT
       'http://www.coveo.com' AS ClickableUri,
       Orders.OrderID AS Title,
       'OrderDate: ' + convert(varchar, OrderDate) + 'RequiredDate: ' + convert(varchar, RequiredDate) + 'ShippedDate: ' + convert(varchar, ShippedDate) + 'Shipped via: ' + Shippers.CompanyName AS Body,
       'Order' AS Type,
       OrderDate,
       RequiredDate,
       ShippedDate,
       Shippers.CompanyName AS Shipper,
       FirstName + ' ' + LastName AS sysAuthor
   FROM
       Orders
   INNER JOIN Shippers ON Orders.ShipVia = Shippers.ShipperID
   INNER JOIN Customers ON Orders.CustomerID = Customers.CustomerID
   INNER JOIN Employees ON Orders.EmployeeID = Employees.EmployeeID
   ``

   - **CES_Products**
   
   Permissions are defined directly as fields inside the view (allowed for all documents is `coveo/hford`).

   ```sql
   CREATE view "CES_Products" AS
   SELECT
       'http://www.coveo.com/Products/details.aspx?Id=' + convert(varchar, Products.ProductID) AS Uri,
       'http://www.coveo.com' AS ClickableUri,
       ProductName + ' (' + convert(varchar, Products.ProductID) + ')' AS Title,
       'Name: ' + ProductName + 'Category: ' + CategoryName + 'Supplier: ' + Suppliers.CompanyName AS Body,
       'Product' AS Type,
       ProductName AS Product,
       Discontinued,
       UnitPrice,
       QuantityPerUnit,
       CategoryName AS Category,
       Suppliers.CompanyName AS Supplier
   FROM
       Categories
       INNER JOIN Products ON Categories.CategoryID = Products.CategoryID
       INNER JOIN Suppliers ON Products.SupplierID = Suppliers.SupplierID
   ```
9.10.6.4 Indexing a Database Using a View

You can index data from a database using embedded views (queries), which are defined directly in your database.

To use embedded views

1. Create a database source (see "Configuring and Indexing a Database Source" on page 869).

2. In your database, create a view that returns at least the URI field (see "Creating a View in a Database" on page 874).

   Note: The URI field value must be a valid URI, meaning it must have any scheme prefix followed by a unique identifier (ex.: odbc://id=4).

The fields that can be mapped to a document are:

- Uri
- UriCaption
- ClickableUri
- PrintableUri
- Title
- FileName
- ContentType
- BinaryBody
- Body
- ModifiedDate
- All security-related fields.

3. Define the required security permissions on your documents using one of the following methods:

   - In the Administration Tool:
     
     Note: No configuration file is required when using this method.

     a. On the Coveo server, access the Administration Tool.
     b. Access the Sources and Collections page (Index > Sources and Collection).
     c. In the Source section, expand the drop-down list of the appropriate source.
     d. Select Edit Permissions. The Permissions page of the selected source is displayed.
     e. Select Specify the security permissions to index.
     f. Specify the necessary users in the Allowed Users and Denied Users lists.
To add a new user, enter the username in the corresponding box and click **Add**. By default the **Allowed Users** list contains *everybody* that has access to the indexed documents.

- Click **Apply Changes**.
  - From the created view:
    - **Note**: No configuration file is required when using this method.
    - In the created view, add new fields containing the required permissions for every document.

<table>
<thead>
<tr>
<th>Security type</th>
<th>User type</th>
<th>Required field names</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>User-related</td>
<td>Server-related</td>
</tr>
<tr>
<td>Windows</td>
<td>Allowed users</td>
<td>AllowedWindowsName</td>
</tr>
<tr>
<td></td>
<td></td>
<td>AllowedWindowsServer</td>
</tr>
<tr>
<td></td>
<td>Denied users</td>
<td>DeniedWindowsName</td>
</tr>
<tr>
<td></td>
<td></td>
<td>DeniedWindowsServer</td>
</tr>
<tr>
<td>Custom group</td>
<td>Allowed users</td>
<td>AllowedCGName</td>
</tr>
<tr>
<td></td>
<td></td>
<td>AllowedCGServer</td>
</tr>
<tr>
<td></td>
<td>Denied users</td>
<td>DeniedCGName</td>
</tr>
<tr>
<td></td>
<td></td>
<td>DeniedCGServer</td>
</tr>
<tr>
<td>Custom user</td>
<td>Allowed users</td>
<td>AllowedCUName</td>
</tr>
<tr>
<td></td>
<td></td>
<td>AllowedCUServer</td>
</tr>
<tr>
<td></td>
<td>Denied users</td>
<td>DeniedCUName</td>
</tr>
<tr>
<td></td>
<td></td>
<td>DeniedCUServer</td>
</tr>
</tbody>
</table>

- On the Coveo server, access the Administration Tool.
- In the **Source** section, expand the drop-down list of the appropriate source.
- Select **Edit Permissions**. The **Permissions** page corresponding to the source is displayed.
- In the **Permissions** section, select **Index security permissions**.

- From a configuration file:
  - Create a configuration file (see "Example of a Configuration File for the Database Connector" on page 860 and "Indexing a Database Using a Configuration File" on page 859).
  - Add an **AllowedUsers** node in which it is possible to define allowed and denied users for every document.

**Note**: Creating a configuration file implies that query expressions have to select the entire view or the required fields.

### 9.10.7 Enabling Multithreading for the Database Connector

The Database connector supports multithreading. This feature can considerably improve performances with subqueries.

To enable multithreading

Specify the number of crawling threads using one of the following methods:
• When configuring a new source

In the Coveo Administration Tool, specify the number of threads in the Add Sources page:

- **Refresh Schedule**: Every day
- **Mail archives configuration file**: 
- **Number of Live Indexing Threads**: 1
- **Max Number of Retries**: 2
- **Number of Refresh Threads**: 2
- **Expand before filtering**: 

**Note**: The peak of performance is between 4 and 6 threads; therefore, setting the value to 200 will have no time benefit.

• Manually (for testing purpose)

When you define the configuration values, add the number of threads as a parameter.

```csharp
m_ConfigValues = new Dictionary<string, string>()
{
    {"ItemType", p_ItemType},
    {"ConfigFile", m_ConfigPath},
    {"DriverType", p_DriverType},
    {"NbRefreshThreads", "1"}
};
```

**Note**: To enable multithreading, NbRefreshThreads must be written as is.

### 9.10.8 Replacing the Identity in Database Connection Strings

In CES, you can create a user identity (see “Adding a User Identity” on page 420) and assign this user identity as well as the connection string to a database source (see "Configuring and Indexing a Database Source" on page 869). When this is done, you can hide the password and user ID in the connection string by respectively introducing the @uid and @pwd tokens. The Database connector internally replaces the tokens with the information provided in the user identity.

**Examples:**

For a basic connection string:

```
Data Source=dbServer.company.com;Initial Catalog=employees;User Id=companyUser;Password=MyPassword
```

Hiding password and user ID using tokens:

```
Data Source=dbServer.company.com;Initial Catalog=employees;User Id=@uid;Password=@pwd
```
Important: You must provide either both tokens or none at all. If you do not provide tokens, but add a user identity, the behavior will be the same as before. The user identity will be used to impersonate the process running the queries.

9.10.9 Enabling Incremental Refresh on a Database Source

Incremental refresh keeps documents up-to-date by scanning repositories and re-indexing modified documents at short intervals. To enable this feature on a database source, database items that have to be indexed, such as tables or views, must contain a date type field to indicate their latest modification date. Fields can be given any name as long as it has the right data type. Furthermore, whenever a record is modified, it is important to update the latest modification date field (see "Configuring and Indexing a Database Source" on page 869 and "Additional XML Attributes" on page 865).

Note: The incremental refresh does not take into account deleted documents. A source full refresh or rebuild is required.

In the SQL query, the SELECT statement must have a WHERE clause with a criterion on the last modification date field.

Example: The following simple example should work with common database engines such as Microsoft SQL Server 2012, PostgreSQL, and MySQL. You must replace [PARAMETER] by @LastRefresh in an SqlClient scenario (MSSQL/SQLServer databases) or by ? otherwise (e.g., NorthWind databases). The [PARAMETER] field is sent by the crawler to the query to indicate when the last increment refresh was performed.

```xml
<Accessor type="query"
   OrderByFieldName="dateCreated"
   OrderByFieldType="DateTime"
   IncrementalRefreshFieldName="dateModified">
   <![CDATA[
      Select id, title, dateModified, content, author 
      FROM blog 
      WHERE dateModified>=[PARAMETER] 
      order by dateModified 
      OFFSET @startRow ROWS FETCH NEXT (@endRow-@startRow) ROWS ONLY;
   ]]> 
</Accessor>
```

The example also includes support for pagination (see OFFSET FETCH Clause (SQL Server Compact)).

What's Next?

Ensure that you also created an incremental refresh schedule on your database source in CES.

9.10.10 Enabling Pause/Resume on a Database Source

The Database connector can support the Pause/Resume parameter if the following is added to your configuration file:
1. In the SQL query, add an ORDER BY on the chronological fields of the SELECT statement:

   **If the source supports Incremental Refresh**
   
   The same chronological fields must also be used in the ORDER BY.

   **If the source does not support Incremental Refresh**
   
   - Field that uniquely identifies each record:
     
     If the primary key contains only one field, select that field. However, if there is a column that contains a sequential number incremented by the DBMS each time a new record is added, select that column instead.
     
     - No field that uniquely identifies each record:
     
       In this case, any field can be used. However, during a resume, records that have been indexed before pausing could be re-indexed.

     **Example:** You have a table containing the 12 months of the year and you select the month column as the reference. The values for this column are not unique, as many rows can be associated to the same month. While crawling the 6th month, you pause, therefore not indexing all the rows for the 6th month. When you resume, the connector will start crawling at the first row of the 6th month, re-indexing the rows that have already been indexed.

2. Add XML attributes on the Accessor element in the configuration file:

   **OrderByFieldName**
   
   Specifies the name of the column on which the ORDER BY is applied. This attribute must be present to enable Pause/Resume.

   **OrderByFieldType**
   
   Specifies the .NET data type of that column. This attribute is not normally required. The connector automatically tries to determine the data type by preparing the SQL query - without however executing it - and looking at the schema of the results. However, if a specific DBMS does not handle that process correctly, you can manually specify the data type with this attribute. The following lists the allowed types:
   
   - short (16-bit signed integer)
   - ushort (16-bit unsigned integer)
   - int (32-bit signed integer)
   - uint (32-bit unsigned integer)
   - long (64-bit signed integer)
   - ulong (64-bit unsigned integer)
   - float (single-precision floating point number)
- double (double-precision floating point number)
- string (String)

**IncrementalRefreshFieldName**

To support both Incremental Refresh and Pause/Resume, IncrementalRefreshFieldName must contain the same name as OrderByFieldName.

Refer to this example for an excerpt of a configuration file for a source with Pause/Resume and Incremental Refresh enabled:

```
<Mapping type="Orders">
  <Accessor type="query"
    OrderByFieldName="OrderDate"
    OrderByFieldType="DateTime"
    IncrementalRefreshFieldName="OrderDate">
    SELECT Shippers.CompanyName AS ShipperName,
      Orders.OrderID AS ID,
      Orders.CustomerID,
      Orders.OrderDate,
      Orders.RequiredDate,
      Orders.ShippedDate,
      Customers.CompanyName,
      Employees.LastName,
      Employees.FirstName
    FROM Orders, Shippers, Customers, Employees
    WHERE Orders.ShipVia = Shippers.ShipperID AND
      Orders.CustomerID = Customers.CustomerID AND
      Orders.EmployeeID = Employees.EmployeeID AND
      Orders.OrderDate >= [PARAMETER]
    ORDER BY Orders.OrderDate
  </Accessor>
</Mapping>
```

**Note:** You must replace [PARAMETER] by @LastRefresh in an SqlClient scenario or by ? otherwise.

**Note:** For backward compatibility, the equivalent LiveIndexingFieldName parameter from previous CES versions is still supported in CES 7.

### 9.10.11 Enabling a Query-Based Security Provider for the Database Connector

You can expand external groups and users using a security provider when the database contains information allowing groups to be expanded to external users and/or external users to be mapped to Active Directory users.

**To expand external groups and users using a security provider**

1. In the source XML mapping file, define `<AllowedUser>` entries with the following properties:
   - **Type (mandatory):** ExternalGroup or ExternalUser.
   - **Name (mandatory):** The name of the external group or user.
     - Supports multiple semicolon (;) separated names.
     - Supports the `%[column]` syntax to use values returned by the Accessor query.
   - **Server/ExpandGroup (mandatory with the ExternalGroup type):** SQL query used by the security provider to expand external groups to external users.
Server/ExpandUser: SQL query used by the security provider to map external users to Active Directory users.

```xml
<AllowedUsers>
  <AllowedUser type="ExternalGroup" allowed="true">
    <Name>%{column_allowed_groups}</Name>
    <Server>
      <ExpandGroup>
        select distinct column_user from membership where column_group = '@GroupName'
      </ExpandGroup>
      <ExpandUser>
        select distinct column_user_nt from nt_account where column_user = '@UserName'
      </ExpandUser>
    </Server>
  </AllowedUser>
</AllowedUsers>
```

2. Create a security provider for your database source (see "Configuring a Database Security Provider" on page 867).

Match the values for the Security provider and Source parameters listed in the following table.

<table>
<thead>
<tr>
<th>Security provider parameter</th>
<th>Source parameter</th>
</tr>
</thead>
<tbody>
<tr>
<td>Driver Type</td>
<td>Driver Type</td>
</tr>
<tr>
<td>Database Connection String</td>
<td>Addresses</td>
</tr>
</tbody>
</table>

3. Associate this new security provider to your database source by selecting it in the Security Provider dropdown list (see Configuring and Indexing a Database Source).

9.10.12 Complement Information Retrieval with Subqueries for the Database Connector

The Database connector acquires information about each indexed document through a query performed against a database. For each query, it is possible to associate one or more subqueries to be executed and used to complement information.

**Example:** You can run a main query, and for each row, run a subquery that crawls more/different information. All the results of a single row from the main query, along with everything from the subquery, are merged into a single document.

The connector requires a mapping file to execute properly. For each mapping type, it is necessary to specify an Accessor representing the SQL query to execute.

9.10.12.1 Specifying Subqueries

To specify subqueries, you must set the type of the Accessor to query.

```xml
<Accessor type="query">

Following the Accessor definition, add an AccessorSubQueries node with all subqueries:
Note: The master key (value following SELECT) in the AccessorSubQuery node must match exactly the one returned by the server. The key you include must also have the same casing. The following error is thrown when the key could not be found:

Unable to index document: There is a formatting error in a sub query. Cannot find master key %[key].

```xml
<AccessorSubQueries>
  <AccessorSubQuery name="FirstNameLastName" separator=";" behaviorOnMultiRows="join" allowDuplicates=false>
    SELECT firstName, lastName
    FROM employeelist
    WHERE Email_id = %[sender]
  </AccessorSubQuery>
</AccessorSubQueries>
```

9.10.12.2 Subquery Attributes

**name**

Subquery name referred to in section Fields of the mapping (see "Example of a Configuration File for the Database Connector" on page 860).

**separator**

Separator used when concatenating multiple rows.

**behaviorOnMultiRows**

Action to take when a subquery returns more than one row. The only supported behavior is join, which concatenates values with the provided separator.

**allowDuplicates (optional)**

This attribute is mainly used when your subquery returns multiple rows. If set to False, duplicates in the results are ignored in the concatenation of the results. If set to true, duplicates are present.

**singleQuoteEscapeSequence (optional)** CES 7.0.5425+ (May 2013)

When the value of the returned field contains single quotes, these single quotes must be escaped. By default when you omit this attribute, the connector escapes the single quotes by doubling them (ex.: "). This escaping mechanism should work in most cases. However, some database types require a different escaping sequence for single quotes. In such cases, use this attribute to specify the single quote escape sequence.

**Example:** For the MySQL database, the single quote escaping sequence is `\'`. In this case, in the AccessorSubQuery tag, include the singleQuoteEscapeSequence attribute as follows:

```xml
<AccessorSubQuery name="FirstNameLastName" separator=";" behaviorOnMultiRows="join"
allowDuplicates="false" singleQuoteEscapeSequence="\\'"/>
```

9.10.12.3 Subquery Master Key

In a subquery, a master key used in the WHERE clause must respect the format %[fieldName], which corresponds to metadata acquired from the main accessor. The master key is used to make the join between the main query and subqueries.
9.10.12.4 Specifying subquery metadata for fields

The `<Fields>` section of the mapping file is used to specify the metadata to use for indexing.

Refer to the following example for a typical `<Fields>` section of a mapping file:

```xml
<Fields>
  <ClickableUri>http://www.coveo.com</ClickableUri>
  <FileName>Message_%[mid].txt</FileName>
  <Title>Message_%[mid]</Title>
  <ModifiedDate> %[date]\</ModifiedDate>
  <Body>%[body]\</Body>
  <CustomFields>
    <CustomField name="sysAuthor">%[sender]</CustomField>
    <CustomField name="firstName">%[FirstNameLastName.firstName]</CustomField>
    <CustomField name="lastName">%[FirstNameLastName.lastName]</CustomField>
  </CustomFields>
</Fields>
```

The metadata of a subquery can be specified for a field or a custom field. The way to specify is similar to the way it is done when referring a field coming from the main accessor: `%(subQueryName.fieldName)`. In the above example, custom field `firstName` is referring subquery named `FirstNameLastName` and uses the `firstName` metadata.

Refer to the following for a complete mapping file, used in our unit tests:

```xml
<?xml version="1.0" encoding="utf-8" ?>
<ODBC>
  <CommonMapping excludedItems="employeelist">
    <AllowedUsers>
      <AllowedUser type="Windows" allowed="true">
        <Name>everyone</Name>
      </AllowedUser>
    </AllowedUsers>
    <Mapping type="message">
      <Accessor type="query">
        SELECT message.mid,
        message.sender,
        message.date,
        message.message_id,
        message.subject,
        message.body,
        message.folder
        FROM message
        WHERE DATE like '2001-04-07%'
      </Accessor>
      <AccessorSubQueries>
        <AccessorSubQuery name="FirstNameLastName" separator=";" behaviorOnMultiRows="join">
          SELECT firstName, lastName
          FROM employeelist
          WHERE Email_id = %[sender]
        </AccessorSubQuery>
      </AccessorSubQueries>
    </Mapping>
  </CommonMapping>
  <Fields>
    <ClickableUri>http://www.coveo.com</ClickableUri>
    <FileName>Message_%[mid].txt</FileName>
    <Title>Message_%[mid]</Title>
    <ModifiedDate> %[date]\</ModifiedDate>
    <Body>%[body]\</Body>
    <CustomFields>
      <CustomField name="sysAuthor">%[sender]</CustomField>
    </CustomFields>
  </Fields>
</ODBC>
```
9.11 Desktop Connector

The Desktop connector allows to index files located on end-user (desktop and laptop) computers connected to your network. The Desktop connector operates together with the Desktop Integration Package (DIP) that, among other features, allows end-users to specify the local folders and mail archive files to be indexed by the Desktop connector.

Once files from the desktop or laptop computer of an end-user are integrated into the Coveo unified index, this end-user (and only this end-user) can search and review the content of his files from any Coveo access point (including from a mobile device) using the Quick View. Because an HTML version of the files is in the unified index, this is true even when the source computer is offline or powered off.

As a Coveo administrator, when you deploy the DIP to end-user computers, you can configure features to be configurable by the end-user, to have fixed values, or to be disabled. Once the content of end-user computers is indexed, you can also manage remote clients from the Administration Tool.

9.11.1 Features

The following details the features available in the Desktop connector:

Security

When crawling files from an end-user computer, the connector indexes file permissions associated to the computer user, ignoring local file and folder sharing permissions that the end-user may have set. This ensures only the computer user can see his files in the search results.

Incremental Refresh

The Desktop connector uses file live monitoring to dynamically look for modifications made to the files on the end-user computer, thus keeping the index synchronized with the content of the computer, without requiring the source to be refreshed.

Mail archives

The Desktop connector can optionally open and index the content of mail archive files from Microsoft Exchange Personal Folders (.pst) and Microsoft Exchange Offline Folders (.ost).

Note: Microsoft Exchange Personal Folders (.pst) files and Microsoft Exchange Offline Folders (.ost) files are referred to as mail archives in the Desktop connector documentation.
DIP client-side configuration

The Desktop connector operates together with the Desktop Integration Package (DIP) that allows end-users to specify the local folders and mail archive files to be indexed by the Desktop connector.

9.11.2 Feature history

<table>
<thead>
<tr>
<th>CES version</th>
<th>Date</th>
<th>Features</th>
</tr>
</thead>
<tbody>
<tr>
<td>7.0.4876+</td>
<td>October</td>
<td>The <strong>Authentication</strong> source parameter is now taken into account (see &quot;Configuring and Indexing a Desktop Connector Source&quot; on page 887) and the <strong>LdapSearchRoot</strong> hidden parameter was added (see &quot;Modifying Hidden Desktop Source Parameters&quot; on page 892) for rare cases where end-users do not have read access to Active Directory.</td>
</tr>
</tbody>
</table>

What's Next?

Review the overview of the deployment process for this connector (see "Desktop Connector Deployment Overview" on page 886).

9.11.3 Desktop Connector Deployment Overview

The following procedure outlines the steps needed to bring content from end-user computers into the Coveo unified index using the Desktop connector. The steps indicate the order in which you must perform the tasks.

1. Validate that your environment meets the requirements (see "Desktop Connector Requirements" on page 886).

2. In the Coveo Administration Tool, create and configure a Desktop source.

   The Desktop connector needs to know details about the end-user computers to be able to index their content (see "Configuring and Indexing a Desktop Connector Source" on page 887).

3. Deploy the Desktop Integration Package (DIP) on end-user computers.

   You need to manage the installation of the DIP on end-user computers using one of the suggested methods (see "Desktop Integration Package Deployment Overview" on page 103).

4. Notify and train end-users to take advantage of the Desktop Integration Package to index local files.

5. Manage remote clients.

   Once the content of end-user computers is indexed, you can centrally manage remote clients from the Administration Tool. You can rebuild, refresh, delete, or disable indexed content from end-user computers (see "Managing Desktop Connector Remote Clients" on page 892).

9.11.4 Desktop Connector Requirements

Your environment needs to meet the following requirements to be able to use the Coveo connector for end-user desktop and laptop computers:

- Coveo license for the Desktop Connector

   Your Coveo license must include support for the Desktop Connector to be able to use this connector.
- Microsoft Windows OS on client-side computers

  The end-user computers must run Microsoft Windows 8 or 7.

  **Note:** Coveo .NET Front-End 12.0.146+ (April 2013) The Desktop Integration Package supports Windows 8.

**What's Next?**

Create and configure a Desktop connector source (see "Configuring and Indexing a Desktop Connector Source" on page 887).

### 9.11.5 Configuring and Indexing a Desktop Connector Source

A Desktop connector source defines a set of configuration parameters determining the end-user computers on the network of your organization from which content can be indexed.

The Desktop connector operates with the Desktop Integration Package (DIP) deployed on end-user computers. The source identifies end-users for which files on desktop and laptop computers that they use should be indexed. The source also identifies the port (1980 by default) on which the connector listens. While the end-user computers are connected to your organization network, the DIP client regularly (every 10 minutes by default) contacts the Coveo server on the Desktop connector port to push new, modified, moved, or deleted local files from the folders specified to be indexed on the computer, thus keeping the index up-to-date.

  **Note:** End-users can configure the local folders to index and review the indexing history from their computer.

It is recommended to create one Desktop source for all your desktop or laptop end-users. If you need to create more than one Desktop source, use a different port for each source and adapt your DIP deployment to use the appropriate port accordingly.

**To configure and index a Desktop connector source**

1. On the Coveo server, access the Administration Tool.
2. Select **Index > Sources and Collections**.
3. In the **Collections** section:
   a. Select an existing collection in which you want to add the new source.
      
      OR
   b. Click **Add** to create a new collection.
4. In the **Sources** section, click **Add**.
   
   The **Add Source** page that appears is organized in three sections.
5. In the **General Settings** section of the **Add Source** page:
a. Enter the appropriate value for the following required parameters:

**Name**

Enter a descriptive name of your choice for the connector source.

**Example:** End-user desktop and laptop computers

**Source Type**

Select the connector used by this source. In this case, select Desktop Connector.

**Note:** If you do not see Desktop Connector, your environment does not meet the requirements (see "Desktop Connector Requirements" on page 886).

**Addresses**

The list of users whose computer content is to be indexed. Enter * to index the content of all end-user computers. Alternatively, enter usernames on separate lines in the form domain\username or username@domain. You can not specify groups.

**Note:** When a user logs to more than one computer on which the DIP is installed and local folders are configured to be indexed, the content from each computer is indexed for this user.

**Refresh Schedule**

Time interval at which the source is automatically refreshed to keep the index content up-to-date. This connector supports incremental refreshes, so the recommended option is either Every Sunday or Every day.
Note: You can create a new (or modify an existing) source refresh schedule.

Example: You can schedule the refresh at lunch time for which chances are higher that many desktop or laptops are powered on and connected to the organization network and, that the indexing will less likely disturb users.

b. Review the value for the following parameters that often do not need to be modified:

Rating
Change this value only when you want to globally change the rating associated with all items in this source relative to the rating of elements in other sources.

Document Types
If you created a custom document type set for this source, select it. Otherwise, select Default.

Active Languages
If you defined custom active language sets, ensure to select the most appropriate for this source.

Fields
If you defined custom field sets, ensure to select the most appropriate for this source.

6. In the Specific Connector Parameters & Options section of the Add Source page, review the default value for the following parameters:

Port
Computer port used by the Desktop Integration Package to communicate with the Desktop connector. The default is 1980 and should not be changed. If you must use another port, you need to deploy the DIP using the GPO method and specify the same port number (see "Configuring the Desktop Integration Package GPO" on page 107).

Maximum active clients
The maximum number of DIP clients from end-user computers that can simultaneously be connected to the Desktop connector. The default value is 50. When the limit is reached, new connection requests are
refused. DIP clients automatically retry 10 minutes later when the Desktop connector refuses a connection.

**Parameters**

Click **Add Parameter** when you want to show advanced source parameters. There are no advanced parameters for this type of connector. The Coveo Support could instruct you to click **Add Parameters** to specify other source parameter names and values that could help to troubleshoot issues.

**Index Subfolders**

This parameter does not apply and is not taken into account by the Desktop source.

**Index the document’s metadata**

When selected, CES indexes all the document metadata, even metadata that are not associated with a field. The orphan metadata are added to the body of the document so that they can be searched using free text queries.

When cleared (default), only the values of system and custom fields that have the **Free Text Queries** attribute selected will be searchable without using a field query.

**Example:** A document has two metadata:

- **LastEditedBy** containing the value Hector Smith
- **Department** containing the value RH

In CES, the custom field CorpDepartment is bound to the metadata Department and its **Free Text Queries** attribute is selected.

When the **Index the document’s metadata** option is cleared, searching for RH returns the document because a field is indexing this value. Searching for hector does not return the document because no field is indexing this value.

When the **Index the document’s metadata** option is selected, searching for hector also returns the document because CES indexed orphan metadata.

**Document’s addresses are case-sensitive**

Leave the check box cleared. This parameter needs to be checked only in rare cases for systems in which distinct documents may have the same name but different casing.

**Generate a cached HTML version of indexed documents**

Select this check box so that at indexing time, CES creates HTML versions of indexed documents. In the search interfaces, end-users can then more rapidly review the content by clicking the **Quick View** link rather than opening the original document with the original application.

For a Desktop source, when the end-user computer is offline or powered off, the Quick View is the only way to review the content of the documents. Consider clearing this check box only if you do not want to use Quick View links or to save resources when building the source.

**Open results with cached version**

Leave this check box cleared (recommended) so that in the search interfaces, the main search result link
opens the original document with the original application. Consider selecting this check box only when you do not want users to be able to open the original document but only see the HTML version of the document as a Quick View. In this case, you must also select **Generate a cached HTML version of indexed documents**.

7. In the **Security** section of the **Add Source** page:

   ![Security Section](image)

   a. In the **Security Provider** drop-down list, select **Active Directory** or a custom Active Directory security provider that you created for a specific domain.

   b. In the **Authentication** drop-down list:

   ```
   Note: CES 7.0.4863–(September 2012) The **Authentication** parameter is not taken into account by the Desktop source. The user identity comes from the DIP clients.
   ```

   - When end-users accounts have read access to Active Directory, select **(none)**.
   - When only specific Windows accounts have read access to Active Directory, select a user identity with credentials that can connect to LDAP to retrieve information on remote clients.

   ```
   Note: When your LDAP server is not the default server, you can use the **LdapSearchRoot** hidden parameter to target a specific LDAP server, port, or path when searching for remote clients accounts (see “Modifying Hidden Desktop Source Parameters” on page 892).
   ```

   ```
   Important: When end-users do not have read access to Active Directory and you do not specify a user identity that has read access, Outlook items (.Pst or .Ost) will be indexed but no mailbox will be assigned to their @sysmailbox field. The consequence is that end-users will not see their emails in the search results. If this situation occurs, set the **Authentication** and the **LdapSearchRoot** parameters appropriately so the LDAP search performed by the Desktop Connector can find the LDAP accounts for all remote clients.
   ```

   c. Click **Save and Start** to save the source configuration and start the indexing of the new source.

   The indexing starts only after the DIP is installed on one or more end-user computers connected to the organization network, and folders to index are configured.

**What's Next?**

Deploy the DIP on end-user computers (see “Desktop Integration Package Deployment Overview” on page 103).
9.11.6 Modifying Hidden Desktop Source Parameters

The **Add Source** and **Source: ... General** pages of the Administration Tool present the parameters with which you can configure the connector for most Desktop setups. More advanced and more rarely used parameters are hidden. You can choose to make one or more of these parameters appear in the **Add Source** and **Source: ... General** pages of the Administration Tool so that you can change their default value. Consider changing values of hidden parameters when you encounter issues.

There is currently only one advanced hidden parameter available with Desktop sources.

**LdapSearchRoot (String)** 7.0.4876+ (October 2012)

Optional LDAP search root parameter used to retrieve information on remote clients (display name, mailbox, etc.). When your LDAP server is not the default server, use this parameter to target a specific LDAP server, port, or path when searching for remote clients accounts.

**Example:** LDAP://OU=Users,DC=corp,DC=acme,DC=com

Use the following procedure only when you want to modify one or more of the above hidden source parameters.

To modify hidden Desktop source parameters

1. Refer to "Adding an Explicit Connector Parameter" on page 450 to add one or more Desktop hidden source parameters.

2. For a new Desktop source, access the **Add Source** page of the Administration Tool to modify the value of the newly added advanced parameter:
   a. Select **Index > Sources and Collections**.
   b. Under **Collections**, select the collection in which you want to add the source.
   c. Under **Sources**, click **Add**.
   d. In the **Add Source** page, edit the newly added advanced parameter value.

3. For an existing Desktop source, access the **Source: ... General** page of the Administration Tool to modify the value of the newly added advanced parameter:
   a. Select **Index > Sources and Collections**.
   b. Under **Collections**, select the collection containing the source you want to modify.
   c. Under **Sources**, click the existing Desktop source in which you want to modify the newly added advanced parameter.
   d. In the **Source: ... General** page, edit the newly added advanced parameter value.

4. Rebuild your Desktop source to apply the changes to the parameters.

9.11.7 Managing Desktop Connector Remote Clients

Once a Desktop source is created, started, and the Desktop Integration Package (DIP) is deployed to end-user computers, you can manage remote DIP clients that are using the Desktop connector. This is done from the
Remote Clients page in the Coveo administrator where you can rebuild, refresh, delete indexed documents, as well as delete and disable remote DIP clients.

To manage remote clients

1. On the Coveo server, access the Administration Tool.

2. Access the Remote Clients page:
   a. Select Index > Sources and Collections.
   b. In the Collections section, select the collection that contains the Desktop source.
   c. In the Sources section, select the Desktop source.
   d. In the navigation panel on the left, click Remote Clients.

3. In the Remote Clients page:
   a. In the Filter box, you can enter text to refine the displayed list of remote DIP clients.
      
      Example: Enter martin in the Filter box to only see clients whose name include martin.
   
   b. Select the check box of one or more remote DIP clients to which you want to apply an action.
   
   c. In the Actions drop-down list, select one of the following actions:
      
      Rebuild

      Select to re-index the whole content of local folders to index, even if nothing has changed. The rebuild takes place as soon as the remote DIP client is connected. In the meantime, the documents remain searchable.
Refresh
Select to only index modified, renamed, or moved documents. The refresh takes place as soon as the remote DIP client is connected. In the meantime, the documents remain searchable.

Delete Documents
Select to remove all indexed documents from the selected remote DIP client computers. Documents will not be searchable until they are re-indexed.

Delete
Select to delete the remote DIP client entry, document count statistics, and all related indexed documents.

Disable
Select to prohibit a remote DIP client from indexing documents.

9.12 Dropbox for Business Connector

The Coveo connector for Dropbox for Business allows Coveo administrators to index and integrate the Dropbox content of their team members into the Coveo unified index. The connector indexes all items and the attached permissions from all team members' Dropboxes so that in the Coveo search interfaces, a user can easily find any but only content to which he has access in Dropbox.

9.12.1 Connector Features Summary

<table>
<thead>
<tr>
<th>Features</th>
<th>Supported</th>
<th>Additional information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dropbox for Business version</td>
<td>Latest cloud version</td>
<td>Following available Dropbox for Business releases</td>
</tr>
<tr>
<td>Searchable content types</td>
<td>✔</td>
<td>Files, folders, and accounts</td>
</tr>
</tbody>
</table>

Content update

<table>
<thead>
<tr>
<th>Incremental refresh</th>
<th>✔</th>
</tr>
</thead>
<tbody>
<tr>
<td>Full refresh</td>
<td>✔</td>
</tr>
<tr>
<td>Rebuild</td>
<td>✔</td>
</tr>
</tbody>
</table>

Document-level security

| ✔ | Dropbox for Business APIs do not return information on shared links [more] |

9.12.2 Features
The Dropbox for Business connector features are:
Content indexing

Extraction and indexing of the following Dropbox for Business item types:

- Folders
- Files
- Accounts

Mostly supported security model

The connector mostly supports the Dropbox for Business security model using a security provider to get almost all permissions for each indexed item. This means that, in Coveo search interfaces, a user searching Dropbox for Business content only sees the content to which he has access except items that he can see using shared links.

*Note:* For the moment, the Dropbox for Business APIs do not return information on shared links.

Incremental refresh

Supports incremental refresh to periodically query Dropbox for the latest edits, keeping the index content up-to-date.

Multithreading

The connector can run multiple threads, which can improve performances considerably (see Modifying Hidden Dropbox for Business Source Parameters).

Pause/Resume

When indexing Dropbox for Business content, the connector can be paused and resumed.

What's Next?

Review the steps to deploy the Dropbox connector (see "Dropbox for Business Connector Deployment Overview" on page 895).

9.12.3 Dropbox for Business Connector Deployment Overview

The following procedure outlines the steps needed to deploy the Dropbox for Business connector. The steps indicate the order in which you must perform configuration tasks on both the Dropbox and Coveo servers.

To deploy the Dropbox for Business connector

1. Validate that your environment meets the requirements (see "Dropbox for Business Connector Requirements" on page 898).
2. On the Dropbox server, authorize the Coveo connector to access the Dropbox of your team members (see "Authorizing the Coveo Connector to Access the Dropbox of Your Team Members" on page 898).
3. On the Coveo server, in the Coveo Administration Tool:
CES 7.0.8047+ (December 2015) Create a user identity

The connector needs to know the access token that you just obtained performing the OAuth 2.0 protocol to connect to your team members Dropbox. You thus need to create a user identity that you will later associate to your Dropbox for Business source (see "Adding a User Identity" on page 420):

i. In the **User** box, enter a value of your choice (i.e., Dropbox for Business).

  **Note:** The User parameter is not used, but cannot be left empty.

ii. In the **Password** box, enter the OAuth 2.0 access token you previously obtained (see Authorizing the Coveo Connector to Access the Dropbox of Your Team Members).

  **Note:** The access token grants the connector access to your team members Dropbox without exposing the administrator's real credentials.

b. Optionally create security providers

When you want to index Dropbox for Business permissions, you must create two security providers to get Dropbox item permissions and resolve and expand groups.

In Dropbox for Business, users are identified by their email addresses. Consequently, permissions returned by the Dropbox for Business security provider for each document are email addresses. The Dropbox for Business security provider then requires another security provider to uniquely identify users from their email addresses.

i. Start by selecting or creating a security provider that the Dropbox for Business security provider will use to resolve and expand groups. The security provider type to use depends on how users are authenticated when they access the search interface:

  **Note:** You may require to also use a REGEX Transform Member Name security provider in between the two following security providers to map member member types. Contact Coveo Support for assistance.

  - When authenticated with their email address, use an Email security provider (see "Configuring an Email Security Provider" on page 65).
  - When authenticated with an Active Directory account, use an LDAP Lookup security provider that maps LDAP identities to Active Directory ones. Contact Coveo Support for assistance.

  **Note:** This chain of security providers is required since the Dropbox security provider does not directly support to be chained with an Active Directory security provider.

ii. Then create a Dropbox for Business security provider that the connector uses to resolve indexed permissions (see "Configuring a Dropbox for Business Security Provider" on page 903).

c. Create a Dropbox field set to take advantage of the available Dropbox metadata.

i. It is recommended to start by importing the default Dropbox field set file [[CES_Path]\Bin\Coveo.CES.CustomCrawlers.Dropbox.FieldSet.xml] to create fields for all the metadata available by default from Dropbox documents.
Note: CES 7.0.8996+ (June 2017) Due to a Dropbox API change, the following fields are removed or filled with a different metadata:

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Status</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>dbtimetaken</td>
<td>Added</td>
<td>Metadata no longer available</td>
</tr>
<tr>
<td>dbdisplaysize</td>
<td>Removed</td>
<td>Metadata no longer available</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Note:</strong> The same information is available in the bytes metadata.</td>
</tr>
<tr>
<td>dbfilelatestrevision</td>
<td>Removed</td>
<td>Always empty since the connector no longer indexes file revisions.</td>
</tr>
<tr>
<td>dbfilename</td>
<td>Removed</td>
<td>Metadata no longer available</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Note:</strong> The same information is available in the Title field.</td>
</tr>
<tr>
<td>dbfoldingchild</td>
<td>Removed</td>
<td>Always empty since the connector no longer indexes file revisions.</td>
</tr>
<tr>
<td>dbicon</td>
<td>Removed</td>
<td>Metadata no longer available</td>
</tr>
<tr>
<td>dbimagetimetaken</td>
<td>Removed</td>
<td>Now merged in dbtimetaken since both fields are based on the same metadata name.</td>
</tr>
<tr>
<td>dbmimetype</td>
<td>Removed</td>
<td>Metadata no longer available</td>
</tr>
<tr>
<td>dbmodifiername</td>
<td>Removed</td>
<td>The item display name is no longer available</td>
</tr>
<tr>
<td>dbvideotimetaken</td>
<td>Removed</td>
<td>Now merged in dbtimetaken since both fields are based on the same metadata name.</td>
</tr>
<tr>
<td>dbfilerevision</td>
<td>Unchanged</td>
<td>No longer available on folders</td>
</tr>
<tr>
<td>dbfilebytes</td>
<td>Updated</td>
<td>Now populated with the size metadata and no longer available on folders</td>
</tr>
<tr>
<td>dbfoldingcollection</td>
<td>Updated</td>
<td>Field values are based on the item URI. Since the URI now uses a different account id, the values of these fields change.</td>
</tr>
<tr>
<td>dbfoldingparent</td>
<td>Updated</td>
<td></td>
</tr>
<tr>
<td>dblastmodificationdate</td>
<td>Updated</td>
<td>Date format changed at the API level, but does not affect the field values. No longer available on folders.</td>
</tr>
</tbody>
</table>

If you have an existing Dropbox for Business source, you must update the field set used by the source, and then rebuild the source to take account of these changes.

ii. When you created custom metadata for your Dropbox documents, add corresponding fields to the field
Configure and index a Dropbox for Business source.

The connector must know details about the authorized access to the Dropboxes of your team members to index their content (see “Configuring and Indexing a Dropbox for Business Source” on page 905).

If you encounter issues, verify if modifying the default value of hidden source parameters can help resolve the problems (see “Modifying Hidden Dropbox for Business Source Parameters” on page 911).

9.12.4 Dropbox for Business Connector Requirements

Your environment must meet the following requirements to be able to use the Dropbox for Business connector:

- CES 7.0.7711+ (June 2015)
- Coveo license for the Dropbox for Business connector

Your Coveo license must include support for the Dropbox for Business connector to be able to use this connector.

- A valid Dropbox for Business account

Using an admin Dropbox for Business account, you must create a Dropbox for Business app in the Dropbox App Console and an OAuth protocol to authorize Coveo to access the Dropbox of your team members (see Authorizing the Coveo Connector to Access the Dropbox of Your Team Members).

What's Next?

Grant Coveo access to the Dropbox of your team members by creating a Dropbox for Business in the App Console (see "Authorizing the Coveo Connector to Access the Dropbox of Your Team Members” on page 898).

9.12.5 Authorizing the Coveo Connector to Access the Dropbox of Your Team Members

You must perform the OAuth 2.0 protocol to authorize the Coveo connector to access the Dropbox content of your team members.

The OAuth 2.0 protocol is a protocol used for granting access to external applications without exposing the user's real credentials. For the connector to be able to connect to your team members Dropbox, it must acquire an access token.

Note: CES 7.0.7711–(June 2015) You can also grant the access to the Dropbox of your team members using the OAuth 1.0 protocol which requires an application key, an application secret, an access token, and an access token secret.

To authorize the Coveo connector to access the Dropbox of your team members

Note: This topic describes a procedure using Google Chrome and the Advanced Rest Client extension. However, it can be done with other browsers and extensions, such as Firefox and the RESTClient plugin.
1. Create an application on a Dropbox for Business account:
   a. Log into the Dropbox website with an administrator account.
   b. Access the Create a new Dropbox for Business app page.
   c. In the Create a new Dropbox for Business app page:
      i. Under What type of app do you want to create?, select the Team member file access check box.
      ii. In the Provide an app name, and you're on your way box, enter a descriptive name of your choice for the application.
         Example: Coveo Business App
   d. In the [Your app name] page:
      i. In the OAuth 2 section, under Generated access token, click Generate.
      ii. Take note of the Access token of your application.
         You need this value when:
         - **CES 7.0.8047+ (December 2015)** Configuring your user identity (see Dropbox for Business Connector Deployment Overview).
         - **CES 7.0.7914– (October 2015)** Configuring your Dropbox for Business security provider and source (see Configuring a Dropbox for Business Security Provider and Configuring and Indexing a Dropbox for Business Source).
         Note: You can now create a Dropbox for Business security provider (see Configuring a Dropbox for Business Security Provider).
   OR
   i. **CES 7.0.7711– (June 2015)** When you want to use the OAuth 1.0, take note of the App key and App Secret of your application. You need these values when configuring your Dropbox for Business security provider and source (see Configuring a Dropbox for Business Security Provider and Configuring and Indexing a Dropbox for Business Source).
      Note: With these two information in hands, you can make API calls to get an OAuth token secret and an OAuth token (see step 2).

2. **CES 7.0.7711– (June 2015)** Make an API call for a request token and a token secret:
   a. Access the Advanced REST client Google Chrome extension page, and then click the + Free button.
      Note: You are asked to download Google Chrome if you did not have the browser installed on your computer already.
b. In the Confirm New App dialog box, click Add.

c. In the Apps page, open the Advanced REST client plugin.

d. In the Request tab:

\[Image of Advanced REST Client plugin with URL and Headers fields\]

i. In the URL box, enter https://api.dropbox.com/1/oauth/request_token.

ii. In the method list, select the POST check box.

iii. Next to Headers, select Raw.

iv. In the box under Headers, copy and paste the following code line after entering your App key and App secret previously obtained in step 1d at the specified places:

\[Authorization: OAuth oauth_version="1.0", oauth_signature_method="PLAINTEXT", oauth_consumer_key="YOURAPPKEY", oauth_signature="YOURAPPSECRET\&".\]

\[Note: Leave the \& sign at the end of your App secret.\]

v. Click Send to receive an answer.

At the bottom of the page, in the Response box, the answer that you receive looks like the following:

\[oauth_token_secret=YOUROAUTHTOKENSECRETVALUE\&oauth_token=YOUROAUTHTOKENVALUE.\]

\[Note: The \& sign is not part of the OAuth token secret.\]

e. Take note of the OAuth token secret and OAuth token values.

3. **CES 7.0.7711– (June 2015)** Authorize your app to use the Dropbox account:
a. Copy and paste the following URL in your browser address bar after entering your OAuth token at the specified place: https://www.dropbox.com/1/oauth/authorize?oauth_token=YOURAUTHTOKENVALUE.

**Note:** If you had an error like the following: This session has expired. Please return to the app to try again, log again in to your admin Dropbox for Business account.

b. In the [Your app name] would like to access [Team name]'s team information and activity log, as well as the ability to perform any action as any team member screen, click Allow to authorize the connector to index the Dropbox content of your team members.

4. **CES 7.0.7711–(June 2015)** Make an API call for an access token and an access token secret:

**Important:** For security reasons, you have a limited time to complete this step before the session expires. If this situation happens, you have to start the procedure over again. Thus, it is recommended to read and understand the procedure before start doing it.
a. Back in the Request tab:

i. In the URL box, enter `https://api.dropbox.com/1/oauth/access_token`.

ii. In the method list, select the POST check box.

iii. Next to Headers, select Raw.

iv. In the box under Headers, copy and paste the following code line after entering your App key, OAuth token, App secret, and OAuth token secret previously obtained at the specified places:

   ```
   Authorization: OAuth oauth_version="1.0", oauth_signature_method="PLAINTEXT",
   oauth_consumer_key="YOURAPPVALUE", oauth_token="YOURAUTHTOKENVALUE",
   oauth_signature="YOURAPPSECRETVALUE&YOURAUTHTOKENSECRETVALUE"
   ```

   **Note:** Leave the `&` sign between the App secret and the OAuth token secret value.

v. Click Send to receive an answer.

   At the bottom of the page, in the Response box, the answer that you receive looks like the following:

   ```
   oauth_token_secret=YOURAUTHTOKENSECRETVALUE&team_id=YOURTEAMIDVALUE&oauth_token=YOURAUTHTOKENVALUE&uid=99026670.
   ```

   **Notes:**
   - The `&` sign is not part of the OAuth token secret value.
   - The `&` sign and the alphanumerical characters beyond are not part of the OAuth token value.

vi. Take note of the OAuth token secret and OAuth token values. You need these values when
configuring your Dropbox for Business security provider and source (see Configuring a Dropbox for Business Security Provider and Configuring and Indexing a Dropbox for Business Source).

What's Next?

Create a Dropbox for Business security provider ("Configuring a Dropbox for Business Security Provider" on page 903).

9.12.6 Configuring a Dropbox for Business Security Provider

The Coveo Dropbox for Business connector mostly supports the Dropbox security model. When you want users searching for Dropbox content in a Coveo search interface to only see the content to which they have access in Dropbox (except items that they can see using shared links), the connector needs a security provider to be able to index the permissions for each indexed Dropbox item.

Notes:

- For the moment, the Dropbox for Business APIs do not return information on shared links.
- You can get familiar with how Coveo components deal with permissions on documents both at indexing and query time.

To configure a Dropbox for Business security provider

1. On the Coveo server, access the Administration Tool.
3. In the navigation panel on the left, click Security Providers.
4. In the Security Providers page, click Add to create a new security provider.
5. In the Modify Security Provider page:
a. Configure the following required parameters:

**Name**

Choose a meaningful name to identify the security provider.

**Example:** Dropbox for Business Security Provider

**Security Provider Type**

In the drop-down list, select **Dropbox for Business (x64)**.

**User Identity**

In the drop-down list, depending on your CES version:

- **CES 7.0.8047+ (December 2015)** Select the user identity that you created previously (see Dropbox for Business Connector Deployment Overview).
- **CES 7.0.7914– (October 2015)** Select (none).

**Security Provider**

Select the security provider that you selected or created to allow this security provider to resolve and expand the groups (see Dropbox for Business Connector Deployment Overview).

**Access Token CES 7.0.7914– (October 2015)**

Enter the access token to use that you previously obtained (see Authorizing the Coveo Connector to
Access the Dropbox of Your Team Members).

Notes:
- The access token is a series of alphanumeric characters.
- CES 7.0.7711–(June 2015) When you choose the OAuth 1.0 authentication method, see OAuth 1.0 Access Token.

b. CES 7.0.7711–(June 2015) (Optional) Click Add Parameter and then use the following hidden parameters when you decide to use the OAuth 1.0 protocol:

ApplicationToken Source
The application token to use that you previously obtained (see Authorizing the Coveo Connector to Access the Dropbox of Your Team Members).

Note: The app key is a series of 15 alphanumeric characters.

ApplicationSecret Source
The application secret to use that you previously obtained (see Authorizing the Coveo Connector to Access the Dropbox of Your Team Members).

Note: The application secret is a series of 15 alphanumeric characters.

AccessTokenSecret Source
The access token secret to use that you previously obtained (see Authorizing the Coveo Connector to Access the Dropbox of Your Team Members).

Note: The access token secret is a series of 15 alphanumeric characters.

c. Leave the Allow Complex Identities cleared as it does not apply to this type of security provider.

d. Click Apply Changes.

What's Next?
Create and index a source (see "Configuring and Indexing a Dropbox for Business Source" on page 905).

9.12.7 Configuring and Indexing a Dropbox for Business Source
A source defines a set of configuration parameters for a specific Dropbox for Business account.
To configure and index a Dropbox for Business source

1. On the Coveo server, access the Administration Tool.
2. Select **Index > Sources and Collections**.
3. In the **Collections** section:
   a. Select an existing collection in which you want to add the new source.
   OR
   b. Click **Add** to create a new collection.
4. In the **Sources** section, click **Add**.
   
   The **Add Source** page that appears is organized in three sections.
5. In the **General Settings** section of the **Add Source** page:

   a. Enter the appropriate value for the following required parameters:

   **Name**

   Enter a descriptive name of your choice for the connector source.

   **Example:** Dropbox for Business
Source Type

Select the connector used by this source. In this case, select Dropbox for Business.

Note: If you do not see Dropbox for Business, your environment does not meet the requirements (see "Dropbox for Business Connector Requirements" on page 898).

Addresses

This parameter is not used, but must not be empty. Enter http://www.dropbox.com.

Fields

Select the field set that you created for your Dropbox for Business source (see Dropbox for Business Connector Deployment Overview).

Refresh Schedule

Time interval at which the index is automatically refreshed to keep the index content up-to-date. By default, the Every day option instructs CES to refresh the source everyday at 12 AM.

Note: Normally the incremental refresh takes care of maintaining the source up-to-date, but due to a Dropbox API limitation, it is recommended to perform a full refresh per day.

Because the incremental refresh takes care of maintaining the source up-to-date, you can select a longer interval such as Every Sunday.

6. In the Specific Connector Parameters & Options section of the Add Source page:

b. Review the value for the following parameters that often do not need to be modified:

Rating

Change this value only when you want to globally change the rating associated with all items in this source relative to the rating to other sources.

Example: When a source replaces a legacy system, you may want to set this parameter to High, so that in the search interface, results from this source appear earlier in the list compared to those from legacy system sources.

Document Types

If you defined a custom document type set for this source, select it.

Active Languages

If you defined custom active language sets, ensure to select the most appropriate for this source.
Specific Connector Parameters & Options

- Index users
- Add Parameter
- Use Subfolders
- Index the document’s metadata
- Generate a cached HTML version of indexed documents
- Open results with cached version

a. CES 7.0.9167+ (December 2017) When you want Dropbox users to be indexed as separate documents, select the following option:

Index Users

b. CES 7.0.8850– (March 2017) (Optional) Select additional content to be indexed using the following option:

Retrieve revisions

Notes:
- Due to a Dropbox API change, this option is no longer supported.
- CES 7.0.8996+ (June 2017) A source rebuild will remove existing indexed file revisions (if any).

Whether file revisions are indexed.

c. CES 7.0.7711– (June 2015) (Optional) Click Add Parameter and then use the following hidden parameters when you decide to use the OAuth 1.0 protocol:

ApplicationToken Security provider

The application token to use that you previously obtained (see Authorizing the Coveo Connector to Access the Dropbox of Your Team Members).

Note: The app key is a series of 15 alphanumeric characters.

ApplicationSecret Security provider

The application secret to use that you previously obtained (see Authorizing the Coveo Connector to Access the Dropbox of Your Team Members).

Note: The application secret is a series of 15 alphanumeric characters.
AccessTokenSecret | Security provider

The access token secret to use that you previously obtained (see Authorizing the Coveo Connector to Access the Dropbox of Your Team Members).

Note: The access token secret is a series of 15 alphanumeric characters.

d. The Option check boxes generally do not need to be changed:

**Index Subfolders**

This parameter is not taken into account for this connector.

**Index the document's metadata**

When selected, CES indexes all the document metadata, even metadata that are not associated with a field. The orphan metadata are added to the body of the document so that they can be searched using free text queries.

When cleared (default), only the values of system and custom fields that have the **Free Text Queries** attribute selected will be searchable without using a field query.

**Example:** A document has two metadata:

- `LastEditedBy` containing the value Hector Smith
- `Department` containing the value RH

In CES, the custom field `CorpDepartment` is bound to the metadata `Department` and its **Free Text Queries** attribute is selected.

When the **Index the document’s metadata** option is cleared, searching for RH returns the document because a field is indexing this value. Searching for hector does not return the document because no field is indexing this value.

When the **Index the document’s metadata** option is selected, searching for hector also returns the document because CES indexed orphan metadata.

**Document's addresses are case-sensitive** [CES 7.0.7711– (June 2015)]

Ensure that this option is selected because Dropbox team member IDs are case sensitive.

**Generate a cached HTML version of indexed documents**

When you select this check box (recommended), at indexing time, CES creates HTML versions of indexed documents. In the search interfaces, users can then more rapidly review the content by clicking the Quick View link rather than opening the original document with the original application. Consider clearing this check box only when you do not want to use Quick View links or to save resources when building the source.

**Open results with cached version**

Leave this check box cleared (recommended) so that in the search interfaces, the main search result link opens the original document with the original application. Consider selecting this check box only when you do not want users to be able to open the original document but only see the HTML version of
the document as a Quick View. In this case, you must also select Generate a cached HTML version of indexed documents.

7. In the Security section of the Add Source page:

   ![Security Provider](image)

   a. When you chose to index Dropbox permissions, in the Security Provider drop-down list, select the Dropbox for Business security provider that you created for this source (see "Configuring a Dropbox for Business Security Provider" on page 903).

   b. CES 7.0.8047+ (December 2015) In the Authentication drop-down list, select the Dropbox for Business user identity that you created for this source (see Dropbox for Business Connector Deployment Overview).

8. Click Save to save the source configuration.

9. When you chose to not index Dropbox permissions, you can set source level permissions that apply to all documents in the source:

   a. In the navigation panel on the left, click Permissions.

   b. In the Permissions page, select Specify the security permissions to index.

   c. In the Allowed Users and Denied Users boxes, enter the users and groups that you respectively want to allow or deny to see search results from this source. The default is to allow everyone \S-1-1-0\ (Active Directory Group).

   d. Click Apply Changes.

10. When you are ready to start indexing the Dropbox for Business source, click Rebuild.

11. Validate that the source building process is executed without errors:

   - In the navigation panel on the left, click Status, and then validate that the indexing proceeds without errors.

     OR

   - Open the CES Console to monitor the source building activities.

What's Next?

Set an incremental refresh schedule for your source.
Consider modifying some hidden source parameters to try resolving other issues (see "Modifying Hidden Dropbox for Business Source Parameters" on page 911).

9.12.7.1 Modifying Hidden Dropbox for Business Source Parameters

The **Add Source** and **Source: ... General** pages of the Administration Tool present the parameters with which you can configure the connector for most Dropbox for Business setups. More advanced and more rarely used parameters are hidden. You can choose to make one or more of these parameters appear in the **Add Source** and **Source: ... General** pages of the Administration Tool so that you can change their default value. Consider changing values of hidden parameters when you encounter issues.

The following list describes the advanced hidden parameters available with Dropbox for Business sources. The parameter type (integer, string, etc.) appears between parentheses following the parameter name.

**ApplicationToken (String)** **Security provider CES 7.0.7711– (June 2015)**

When using the OAuth 1.0 protocol, the application token to use that you previously obtained (see Authorizing the Coveo Connector to Access the Dropbox of Your Team Members).

*Note: The app key is a series of 15 alphanumeric characters.*

**ApplicationSecret (String)** **Security provider CES 7.0.7711– (June 2015)**

When using the OAuth 1.0 protocol, the application secret to use that you previously obtained (see Authorizing the Coveo Connector to Access the Dropbox of Your Team Members).

*Note: The application secret is a series of 15 alphanumeric characters.*

**AccessTokenSecret (String)** **Security provider CES 7.0.7711– (June 2015)**

When using the OAuth 1.0 protocol, the access token secret to use that you previously obtained (see Authorizing the Coveo Connector to Access the Dropbox of Your Team Members).

*Note: The access token secret is a series of 15 alphanumeric characters.*

**NumberOfRefreshThreads (Integer)**

The number of refresh threads used by the crawler for this source. The default value is 4.

To modify hidden Dropbox for Business source parameters

1. Refer to "Adding an Explicit Connector Parameter" on page 450 to add one or more Dropbox for Business source parameters.

2. For a new Dropbox for Business source, access the **Add Source** page of the Administration Tool to modify the value of the newly added advanced parameter:
   a. Select **Index > Sources and Collections**.
   b. Under **Collections**, select the collection in which you want to add the source.
c. Under Sources, click Add.

d. In the Add Source page, edit the newly added advanced parameter value.

3. For an existing Dropbox for Business source, access the Source: ... General page of the Administration Tool to modify the value of the newly added advanced parameter:

   a. Select Index > Sources and Collections.

   b. Under Collections, select the collection containing the source you want to modify.

   c. Under Sources, click the existing Dropbox for Business source in which you want to modify the newly added advanced parameter.

   d. In the Source: ... General page, edit the newly added advanced parameter value.

4. Rebuild your Dropbox for Business source to apply the changes to the parameters.

9.13 EMC Documentum Connector

The Documentum connector allows Coveo administrators to bring the content of EMC Documentum repository into the unified index so that it becomes searchable by end-users.

The features of the Documentum connector are:

**Content indexing**

- The connector can retrieve and index exclusively all EMC Documentum repository content.

**Fully supported security model**

- The connector supports the EMC Documentum security model by indexing EMC Documentum item permissions so that in Coveo search interfaces, a user searching EMC Documentum content only sees the content to which he has access in EMC Documentum.

**Incremental refresh**

- Periodically queries EMC Documentum Content Server for the latest repository edits, keeping the index content up-to-date.

**Feature history**

<table>
<thead>
<tr>
<th>CES version</th>
<th>Monthly release</th>
<th>Features</th>
</tr>
</thead>
<tbody>
<tr>
<td>7.0.5031</td>
<td>March 2013</td>
<td>Supports multi-value fields</td>
</tr>
</tbody>
</table>

What's Next?

Review the steps to deploy the Documentum connector (see "EMC Documentum Connector Deployment Overview" on page 913).
9.13.1 EMC Documentum Connector Deployment Overview

The following procedure outlines the steps needed to deploy the EMC Documentum connector. The steps indicate the order in which you must perform configuration tasks on both EMC Documentum and Coveo servers.

1. Validate that your environment meets the requirements (see "EMC Documentum Connector Requirements" on page 913).
2. On Documentum Administrator, create a user with read permissions to all Documentum repositories content and security permissions to be used as a crawling account.
3. On the Coveo server:
   a. Create a user identity.
      The Coveo connector needs an account to crawl your EMC Documentum content. For this purpose, select an existing EMC Documentum account or create a new one that has read access to all the content that you want to index (see "Adding a User Identity" on page 420).
   b. Create a security provider.
      When you want to index permissions, you must configure a security provider (see "Configuring an EMC Documentum Security Provider" on page 914).
   c. Configure and index the Documentum source.
      The Coveo connector needs to know details about your EMC Documentum instance to be able to index its content (see "Configuring and Indexing an EMC Documentum Source" on page 916).
   d. If you encounter issues, verify if modifying the default value of hidden source parameters can help resolve the problems (see "Modifying Hidden EMC Documentum Source Parameters" on page 921).

9.13.2 EMC Documentum Connector Requirements

Your environment needs to meet the following requirements to be able to use the Coveo connector for end-user desktop and laptop computers:

- Coveo license for the Documentum Connector
  Your Coveo license must include support for the Documentum connector to be able to use this connector.

- EMC Documentum Content Server version:
  - Supported versions: 7.0
  - Deprecated support versions: 5.3 to 6.7

- The equivalent version of EMC Documentum Foundation Classes must be installed on the server hosting CES.

  **Note:** Ensure your Coveo Master server meets the EMC Documentum Foundation Classes requirements.

  **Example:** If you use EMC Documentum Content Server 6.7, you must install EMC Documentum Foundation Classes 6.7.

- (For Documentum 6.5 to 7.0) Java Runtime Environment 7 (JRE) 32-bit.
Note: Ensure that the path to JRE 7 is in the environment variable named Path. If not, add the path (see “Troubleshooting EMC Documentum Connector Issues” on page 922).

Example: When you use Documentum 7.0, the JRE 7 path should like the following:

C:\Program Files (x86)\Java\jre7\bin\client

What's Next?

Create and configure a Documentum connector source (see “Configuring and Indexing an EMC Documentum Source” on page 916).

9.13.3 Configuring an EMC Documentum Security Provider

When you choose to index permissions associated with EMC Documentum items, the Coveo connector needs a security provider. When permissions are indexed, in Coveo search results, a user searching for EMC Documentum Server content only sees the content to which he has access in EMC Documentum.

Note: You can get familiar with how Coveo components deal with permissions on documents both at indexing and query time.

To configure a Documentum security provider

1. On the Coveo server, access the Administration Tool.
3. In the navigation panel on the left, click Security Providers.
4. In the Security Providers page, click Add to create a new security provider.
5. In the Modify Security Provider page:
a. Configure the following required parameters:

**Name**

Choose a significant name to identify the security provider.

*Example: Documentum7 Security Provider*

**Security Provider Type**

Select Documentum (x86).

**User Identity**

Select the Documentum user identity that you created previously.

**Active Directory Security Provider**

When the user names in your Documentum instance match the usernames in your Active Directory (AD) and you want to allow AD users to see Documentum items in search results, in the drop-down list, select Active Directory to allow this Documentum security provider to map Documentum permissions to AD users.

*Note: If your Documentum and AD usernames do not match, contact Coveo Support for assistance with other methods to map users or use the ForceADDomain hidden parameter.*
b. (Optional) Click **Add Parameter** and then use the following hidden parameter when you want to match your Documentum usernames to their Windows usernames:

**ForceADDomain CES 7.0.5031+ (March 2013)**

Enter a value to overwrite the domain value when CES expands users to Windows users. The default value is **null**.

**Example:** When the **ForceADDomain** parameter value is **MyCompany** and you expand the Documentum user **John**, the security provider will expand this user to the AD user **MyCompany\John**.

c. Leave the **Allow Complex Identities** cleared as it does not apply to this type of security provider.

d. Click **Apply Changes**.

What's Next?

Configure and index a Documentum source (see "Configuring and Indexing an EMC Documentum Source" on page 916).

9.13.4 Configuring and Indexing an EMC Documentum Source

A source defines a set of configuration parameters for a specific EMC Documentum repository. When you want to index more than one EMC Documentum repository, configure one source for each repository.

To configure and index a source with the Documentum connector

1. On the Coveo server, access the Administration Tool.
2. Select **Index > Sources and Collections**.
3. In the **Collections** section:
   a. Select an existing collection in which you want to add the new source.

   OR

   b. Click **Add** to create a new collection.
4. In the **Sources** section, click **Add**.
5. In the **General Settings** section of the **Add Source** page:
a. Enter the appropriate value for the following required parameters:

**Name**

Enter a descriptive name of your choice for the connector source.

**Example:** Documentum7

**Source Type**

The connector used by this source. In this case, select **Documentum**.

**Addresses**

Depending on the EMC Documentum server repository(ies) or the part of a repository you want to index:

**Note:** By default, subfolders are indexed. To index only the main folder, clear the **Index subfolders** option (see "Index Subfolders" on page 920).

- To index all the repositories known to the docBroker, enter `svr-documentum`, which is host of the docbroker, as written in the `dmcl.ini` file of the Documentum installation.
- To only index the `documentum_repo` repository: `svr-documentum/documentum_repo`.
- **CES 7.0.4887+ (November 2012)** To only index specific part of a repository, you can use custom DQL queries that respect the following format:
DQL:<docbaseName>: Where <my conditions>

Examples:
- DQL:DEVCOMPANYXYZ:Where 0."object_name" = 'mydocument.txt'
- DQL:DEVCOMPANYWXYZ:Where FOLDER('/CabinetA/FolderA', DESCEND)

Fields

If you created a custom EMC Documentum field set, select it. Otherwise, leave the Default Scheme.

**Note:** CES 7.0.5031+ (March 2013) Support for multi-value fields, which are separated with a ; character.

Refresh Schedule

Time interval at which the index is automatically refreshed to keep the index content up-to-date. By default, the Every day option instructs CES to refresh the source everyday at 12 AM.

b. Review the value for the following parameters that often do not need to be modified:

Rating

Change this value only when you want to globally change the rating associated with all items in this source relative to the rating to other sources.

**Example:** If this source was for a legacy Lithium community, you may want to set this parameter to Low, so that in the search interface, results from this source appear later in the list compared to those from other sources.

Document Types

If you defined custom document type sets, ensure to select the most appropriate for this source.

Active Languages

If you defined custom language sets, ensure to select the most appropriate for this source.

6. In the Specific Connector Parameters & Options section of the Add Source page:
a. Enter the appropriate value for the following required parameters:

**Webtop folder name**

Enter the name of the EMC Documentum Webtop installation folder. Webtop is the web-based application through which CES accesses EMC Documentum content.

*Example: When Webtop is accessed using the following URL: http://svr-documentum:8080/webtop/, the Webtop folder name is webtop.*

**Webtop host machine name**

Enter the name of the machine on which the EMC Documentum Webtop installation folder is located.

*Example: When your Webtop URL is http://svr-documentum:8080/webtop/, the Webtop host machine name is svr-documentum.*

**Webtop host port number**

Enter the number of the port used by the Webtop application. The default port number is 1489.

*Example: When webtop URL is http://svr-documentum:8080/webtop/, the Webtop host port number is 8080.*

b. Review if you need to change the default value for the following parameter:

**Index All Versions**

Indicates whether to index all versions of a document found on the Documentum server or just the most recent one.

c. In the Parameters section, click Add Parameter to be able to change the default value of hidden parameters (see "Modifying Hidden EMC Documentum Source Parameters" on page 921).

d. In the Option section, review the default value of the following check boxes:
Index Subfolders

Check to index all subfolders below the specified Lithium server address. Selected by default.

Index the document's metadata

When selected, CES indexes all the document metadata, even metadata that are not associated with a field. The orphan metadata are added to the body of the document so that they can be searched using free text queries.

When cleared (default), only the values of system and custom fields that have the Free Text Queries attribute selected will be searchable without using a field query.

Example: A document has two metadata:

- LastEditedBy containing the value Hector Smith
- Department containing the value RH

In CES, the custom field CorpDepartment is bound to the metadata Department and its Free Text Queries attribute is selected.

When the Index the document's metadata option is cleared, searching for RH returns the document because a field is indexing this value. Searching for hector does not return the document because no field is indexing this value.

When the Index the document's metadata option is selected, searching for hector also returns the document because CES indexed orphan metadata.

Generate a cached HTML version of indexed documents

When you select this check box (recommended), at indexing time, CES creates HTML versions of indexed documents. In the search interfaces, users can then more rapidly review the content by clicking the Quick View link rather than opening the original document with the original application. Consider clearing this check box only if you do not want to use Quick View links or to save resources when building the source.

Open results with cached version

Leave this check box cleared (recommended) so that in the search interfaces, the main search result link opens the original document with the original application. Consider selecting this check box only when you do not want users to be able to open the original document but only see the HTML version of the document as a Quick View. In this case, you must also select Generate a cached HTML version of indexed documents.

7. In the Security section of the Add Source page:
In the **Authentication** drop-down list:

- When you want to index secured EMC Documentum content, select the user identity that you created for this source (**EMC Documentum Connector Deployment Overview**).
  
  OR

- When you want to index public content, select **(none)**.

b. Click **Save** to save the source configuration.

8. On the toolbar, click **Start/Rebuild** to start indexing your source.

9. Validate that the source building process is executed without errors:

   - In the navigation panel on the left, click **Status**, and then validate that the indexing proceeds without errors.

   OR

   - Open the CES Console to monitor the source building activities.

What's Next?

Consider modifying advanced source parameters (see "Modifying Hidden EMC Documentum Source Parameters" on page 921).

9.13.4.1 Modifying Hidden EMC Documentum Source Parameters

The **Add Source** and **Source: ... General** pages of the Administration Tool present the parameters with which you can configure the connector for most EMC Documentum setups. More advanced and more rarely used parameters are hidden. You can choose to make one or more of these parameters appear in the **Add Source** and **Source: ... General** pages of the Administration Tool so that you can change their default value. Consider changing values of hidden parameters when you encounter issues.

The following list describes the advanced hidden parameters available with EMC Documentum sources. The parameter type (integer, string…) appears between parentheses following the parameter name.

**DocuApiTimeoutInSeconds (Integer)**

The timeout value (in seconds) allowed for CES to connect with the Documentum API. By default, there is no timeout value. Set it to 60s when debugging.
DocIndexAllDocumentLocations (Boolean)

Whether to create one CES document per document location. The default value is true. Set the value to false when you do not want to index a document more than once even if the document is located in more than one location.

IncrementalRefreshDeletedDocuments (Boolean)

Indicates whether to look for deleted documents during an incremental refresh. The default is true. Set the value to false when you want to keep deleted documents in your index.

Use the following procedure only when you want to modify one or more of the above hidden source parameters.

To modify hidden EMC Documentum source parameters

1. Refer to "Adding an Explicit Connector Parameter" on page 450 to add one or more EMC Documentum hidden source parameters.

2. For a new EMC Documentum source, access the Add Source page of the Administration Tool to modify the value of the newly added advanced parameter:

   a. Select Index > Sources and Collections.
   b. Under Collections, select the collection in which you want to add the source.
   c. Under Sources, click Add.
   d. In the Add Source page, edit the newly added advanced parameter value.

3. For an existing EMC Documentum source, access the Source: ... General page of the Administration Tool to modify the value of the newly added advanced parameter:

   a. Select Index > Sources and Collections.
   b. Under Collections, select the collection containing the source you want to modify.
   c. Under Sources, click the existing EMC Documentum source in which you want to modify the newly added advanced parameter.
   d. In the Source: ... General page, edit the newly added advanced parameter value.

4. Rebuild your EMC Documentum source to apply the changes to the parameters.

9.13.5 Troubleshooting EMC Documentum Connector Issues

Load JVM DLL Failed on LoadLibrary

The pop-up window containing this error message is only available when running Coveo Enterprise Search 7 x [version] as a standalone application:

1. Right-click Command Prompt, and then select Run as administrator.

2. Run CES 7 x[version] as a standalone application using a command line like the following: "C:\Program Files\Coveo Enterprise Search 7\Bin\CESService7.exe" -standalone -port 52800.
Possible causes

- You did not have Java Runtime Environment 7 (JRE 7) 32-bit installed on the machine hosting EMC Documentum.
- The path to JRE 7 32-bit is not in the environment variable named Path.

Possible solution

1. Stop the CES service.
2. Access the System Properties window:
   a. Right-click the Windows Start button, and then select Control Panel.
   b. In the Control Panel window, click System and Security.
   c. In the System and Security window, click System.
   d. In the System window, in the navigation bar on the left, click Advanced system settings.
3. In the System Properties window, click Environment Variables....
4. In the Environment Variables window, under System variables, select the Path variable, and then click Edit....
5. Ensure that Variable value box contains the path to the right JRE version.
   
   Example: When you use Documentum 7.0, the path should like the following:
   
   C:\Program Files (x86)\Java\jre7\bin\client

6. Click OK.
7. Restart the CES service.

9.14 EPiServer CMS Connector

Deprecated

The Coveo prototype connector for EPIserver CMS systems allows you to index the content of one or more EPIserver CMS servers, integrating that content into the Coveo unified index, and making it easily searchable by users.

Note: As of March 2, 2017, the EPIserver CMS connector is deprecated (see "What Does Deprecated Mean for a Coveo Connector?" on page 739).

9.14.1 Features

The following details the features available in the EPIserver CMS connector:

Content Indexing

The connector can retrieve and index exclusively the content of the following EPIserver CMS elements:
- Pages
- Documents
- Downloadable files available from the File Manager

Limitations

This prototype connector does not support:

- Incremental refresh (but does support scheduled source refresh)
- Permissions

What's Next?

Review the deployment process (see “EPiServer CMS Connector Deployment Overview” on page 924).


The following procedure outlines the tasks needed to deploy the Coveo prototype connector for EPiServer CMS systems. The tasks indicate the order in which you must perform key configurations on both the EPiServer CMS and Coveo systems. When needed, the steps refer to a detailed procedure.

To deploy the EPiServer CMS connector

1. Validate that your environment meets the requirements (see “EPiServer CMS Connector Requirements” on page 925).

2. Get and install the EPiServer CMS prototype connector files.

   The connector files are not distributed with the CES installation (see “Getting the EPiServer CMS Connector Files” on page 925).

3. On the EPiServer CMS system, configure the Coveo Web service.

   The connector uses Coveo Web service files that you must copy on the EPiServer CMS server (see “Configuring the Coveo Web Service on an EPiServer CMS Server” on page 926).

4. Configure the user identity.

   The connector needs an account to connect to the EPiServer CMS system and access the entire content that you want to index (see “Adding a User Identity” on page 420).

5. Configure and index the EPiServer CMS source.

   The connector needs to know details about the EPiServer CMS source to be able to index its content (see "Configuring and Indexing an EPiServer CMS Source" on page 928).

6. Optional tasks:

   a. Configure the connector to index the content of the EPiServer CMS File Manager.
You can also index the content of the downloadable files stored in the EPiServer CMS File Manager by specifying which starting addresses to crawl (see "Configuring the EPiServer CMS Source to Crawl the File Manager" on page 932).

b. Create and use a configuration file.

You can instruct the connector to index linked files using a configuration file (see "Creating and Using an EPiServer CMS Configuration File" on page 933).

c. Create and use a custom mapping file.

You can customize how the connector maps metadata to Coveo fields using a custom mapping file (see "Creating and Using an EPiServer CMS Mapping File" on page 934).

d. Add hidden source parameters.

You can use a few hidden source parameters to fine tune how the connector operates (see "Modifying Hidden EPiServer CMS Source Parameters" on page 936).

9.14.3 EPiServer CMS Connector Requirements

Your environment must meet the following requirements to be able to use the Coveo connector for EPiServer CMS systems:

- Coveo EPiServer CMS Connector package
  The files associated with the Coveo prototype connector for EPiServer CMS systems are not available with the default CES installation. Contact the Coveo Support to get the EPiServer CMS package.

- EPiServer CMS version 6
  The connector was developed and tested with EPiServer CMS version 6.1.

What’s Next?

Add the connector to CES (see "Getting the EPiServer CMS Connector Files" on page 925).

9.14.4 Getting the EPiServer CMS Connector Files

The Coveo prototype connector for EPiServer CMS systems is not available by default with the default CES installation. Because it is a prototype, the files associated with the connector are not distributed with the CES installation. Before being able to use the connector, you must get the EPiServer CMS files, copy associated files to your CES implementation, and let CES know where to find them.

To add the EPiServer CMS connector to CES

1. Contact the Coveo Support, to get the EPiServer CMS files specifying if you are using a 32-bit or 64-bit server:
   - Coveo.CES.CustomCrawlers.EpiServer.dll
   - Coveo.Connectors.EpiServer.dll
   - Coveo.Connectors.EpiServer.CoveoService.zip that contains:
2. Copy the following files:
   - Coveo.CES.CustomCrawlers.EpiServer.dll
   - Coveo.Connectors.EpiServer.dll

3. On the Coveo Master server, paste the two files to the [CES_Path]\Bin folder.

4. Add the EPiServer CMS connector to the list of CES connectors using the following information in the Modify Additional Connector page (see "Adding a Connector" on page 444):
   - **Name**: EPiServer
   - **Assembly Path**: Coveo.CES.CustomCrawlers.EpiServer.dll
   - **Type Name**: Coveo.CES.CustomCrawlers.EpiServer.EpiServerCrawler
   - **Run in 64 bits**: On a 64-bit server, when you use the 64-bit version of the connector files, ensure to select this check box.
   - **Parameter**: Apart from required parameters (see "Adding a Connector" on page 444), you can also expose some hidden parameters (such as the optional ConfigFile and MappingFile) by adding them here. You can get the parameter types and names from the list of hidden parameters (see "Modifying Hidden EPiServer CMS Source Parameters" on page 936).

What's Next?

Configure the Web service on the EPiServer CMS server (see "Configuring the Coveo Web Service on an EPiServer CMS Server" on page 926).

9.14.5 Configuring the Coveo Web Service on an EPiServer CMS Server

The Coveo connector for EPiServer CMS systems uses Web services that are inactive by default on an EPiServer CMS system. You must activate them for the account that you want to use to crawl the EPiServer CMS content. You must also deploy the Coveo Web service files on the EPiServer CMS server.

To configure the Coveo Web service for an EPiServer CMS server

1. Activate the Web service:
   a. Using an administrator account, log in to the EPiServer CMS site.
   b. Right-click anywhere on the content, and then select **Admin Mode** in the contextual menu.
c. In the panel on the left:
   i. Click the **Config** tab.
   ii. Under **Security**, click **Permissions for Functions**.

d. In the **Permissions for Functions** panel on the right:
   i. Click **Edit** next to **Allow the user to act as a web service user**.
   ii. Click **Add Users/Groups**.
   e. In the **Add Users/Groups** dialog box, add the account that you selected to use to crawl the EPiServer CMS content, and then click **OK**.
   f. Back in the **Permissions for Functions** panel on the right, click **Save**.

2. Deploy the Coveo Web service files on the EPiServer CMS server:

b. Paste the file in the WebServices folder of the EPiServer CMS installation (not on the Website). This file basically points to the CoveoService.dll, which will be loaded in the Web services of the EPiServer CMS site.

Example: When EPiServer CMS is installed using the default installation folder, the full path of the file is similar to C:\Program Files (x86)\EPiServer\CMS\6.1.379.0\Application\WebServices\CoveoService.asmx.

Note: You can save the CoveoService.asmx in another folder and use the WebServiceUrl hidden parameter to specify the folder (see "Modifying Hidden EPiServer CMS Source Parameters" on page 936).

c. From the EPiServer CMS package, copy the CoveoService.dll file.

d. Paste the file in the bin folder of the EPiServer CMS website that you want to crawl.

Example: When EPiServer CMS sites are installed using default installation folders, the full path to the file is similar to C:\EPiServer\Sites\MyEPiServerSite\bin\CoveoService.dll.

e. On the EPiServer CMS server, reset IIS.

What's Next?

The Coveo connector needs an account to connect to the EPiServer CMS system and access the entire content that you want to index (see "Adding a User Identity" on page 420).

9.14.6 Configuring and Indexing an EPiServer CMS Source

A source defines a set of configuration parameters for a specific EPiServer CMS server.

Note: In an environment with more than one EPiServer CMS servers, define one source for each EPiServer CMS server that you want to index.

To configure and index an EPiServer CMS source

1. On the Coveo server, access the Administration Tool.

2. Select Index > Sources and Collections.

3. In the Sources section, click Add.

4. In the Collections section:
   a. Select an existing collection in which you want to add the new source.

      OR

   b. Click Add to create a new collection.

5. In the General Settings section of the Add Source page:
a. Enter the appropriate value for the following required parameters:

**Name**

A descriptive name of your choice for the connector source.

**Example**: EPiServer CMS

**Source Type**

The connector used by this source. In this case, select EPiServer.

**Note**: If you do not see the EPiServer option, ensure that you obtained the connector files and added the connector to CES (see "Getting the EPiServer CMS Connector Files" on page 925).

**Addresses**

The root address of the EPiServer CMS application in the http://[EPiServer-host]:[port]/form.

**Example**: http://MyEpiServer:17002/

b. The following parameters generally do not need to be changed:

**Rating**

Change this value only when you want to globally change the rating associated with all items in this source relative to the rating to other sources.
**Example:** When a source replaces a legacy system, you may want to set this parameter to **High**, so that in the search interface, results from this source appear earlier in the list compared to those from legacy system sources.

**Document Types**

If you defined a custom document type set for this source, select it.

**Active Languages**

If you defined custom active language sets, ensure to select the most appropriate for this source.

**Fields**

If you defined custom field sets, ensure to select the most appropriate for this source.

**Refresh Schedule**

Time interval at which the index is automatically refreshed to keep the index content up-to-date. By default, the **Every day** option instructs CES to refresh the source everyday at 12 AM.

Because incremental refresh is not available for the EPiServer CMS prototype connector, ensure to select an appropriate source refresh schedule, as this is the only mechanism that ensures that the index content is kept up-to-date.

**Note:** You can create new or modify existing source refresh schedules.

**Parameter**

Click **Add Parameter** when you want to show advanced source parameters (see "Modifying Hidden EPiServer CMS Source Parameters" on page 936).

6. In the **Specific Connector Parameters & Options** section of the **Add Source** page, review the **Option** check boxes that generally do not need to be changed:

- **Index Subfolders**
  - Keep this check box selected (recommended). By doing so, all subfolders from the specified portal address are indexed.

- **Index the document's metadata**
  - When selected, CES indexes all the document metadata, even metadata that are not associated with a field. The orphan metadata are added to the body of the document so that they can be searched using free
text queries.

When cleared (default), only the values of system and custom fields that have the **Free Text Queries** attribute selected will be searchable without using a field query.

**Example:** A document has two metadata:

- **LastEditedBy** containing the value Hector Smith
- **Department** containing the value RH

In CES, the custom field CorpDepartment is bound to the metadata Department and its **Free Text Queries** attribute is selected.

When the **Index the document's metadata** option is cleared, searching for RH returns the document because a field is indexing this value. Searching for hector does not return the document because no field is indexing this value.

When the **Index the document's metadata** option is selected, searching for hector also returns the document because CES indexed orphan metadata.

**Document's addresses are case-sensitive**

Leave the check box cleared. This parameter needs to be checked only in rare cases for systems in which distinct documents may have the same name but different casing.

**Generate a cached HTML version of indexed documents**

When you select this check box (recommended), at indexing time, CES creates HTML versions of indexed documents. In the search interfaces, users can then more rapidly review the content by clicking the Quick View link rather than opening the original document with the original application. Consider clearing this check box only when you do not want to use Quick View links or to save resources when building the source.

**Open results with cached version**

Leave this check box cleared (recommended) so that in the search interfaces, the main search result link opens the original document with the original application. Consider selecting this check box only when you do not want users to be able to open the original document but only see the HTML version of the document as a Quick View. In this case, you must also select **Generate a cached HTML version of indexed documents**.

7. In the **Security** section of the **Add Source** page:
a. In the Security Provider drop-down list, select an Active Directory security provider.

b. In the Authentication drop-down list, select the user identity that you created for the EPiServer source (see “Adding a User Identity” on page 420).

c. Click Save.

8. In the navigation panel on the left, click General.

9. In the General page:

a. Modify the Title Selection Sequence so that the Use the filename option is the first option at the top of the list.

b. Click Apply Changes.

10. When you are ready to start indexing the EPiServer CMS source, click Start.

11. In the navigation panel on the left, click Status, and then validate that the indexing process runs without errors.

9.14.7 Configuring the EPiServer CMS Source to Crawl the File Manager

The File Manager is an EPiServer CMS section where all the files uploaded to the EPiServer CMS installation reside. It is a virtual file system hosted in the Web server. The Coveo connector can access these files through the Coveo Web service.

Example: You may want to crawl and index the content of the File Manager because it contains files that are not referenced from any pages so that users will be able to search for their content.

You instruct the connector to index the File Manager by adding the FileManagerConfigurationString hidden parameter to the EPiServer CMS source. The value of this parameter is the configuration string that contains the list of starting points to crawl in the File Manager.

Each starting point represents a virtual path provider, which gives access to the files it hosts. In the configuration string, each starting point is composed of two values:

- Virtual path provider Name
- Virtual path provider VirtualPath

You can find these values in the episerver.config file associated with the EPiServer CMS website that you are crawling.
Note: When you want to index only downloadable documents referred from links in pages, you should rather use an optional configuration file to instruct the connector to do so (see "Creating and Using an EPiServer CMS Configuration File" on page 933).

To configure the EPiServer CMS source to crawl the File Manager

1. Identify the starting points that you want to crawl in the EPiServer CMS File Manager:
   a. Using a text editor, open the episerver.config configuration file for the EPiServer website that you are crawling.
      
      Example: For the MyEPiServerSite site the file can be in C:\EPiServer\Sites\MyEPiServerSite\episerver.config.

   b. In the configuration file, look for the <virtualPath> node.

   c. Inside this node, look for the <providers> node that contains <add ...> nodes, one for each starting point.

   d. For each starting point that you want to crawl note the values of the Name and VirtualPath attributes.

2. Build the configuration string specifying the starting points to crawl:
   a. For each starting point, directly concatenate the values of the Name and VirtualPath attributes.

   b. Separate starting point strings by a semicolon character.

   Example: The default starting point Documents in EPiServer CMS has the following Name=SiteDocuments and VirtualPath=~/Documents/ attribute values. The default starting point Global Files has the Name=SiteGlobalFiles and VirtualPath=~/Global/ attribute values. The resulting string to crawl both starting points is: SiteDocuments~/Documents;SiteGlobalFiles~/Global/.

3. Add the FileManagerConfigurationString hidden parameter to the EPiServer CMS source and use the string built in the previous step for the parameter value (see "Modifying Hidden EPiServer CMS Source Parameters" on page 936).


You can optionally create and use a configuration file with an EPiServer CMS source. The purpose of the configuration file is to specify fields that are links to downloadable documents that you want to index. Without a configuration file, the connector crawls the content of the pages but not the content of downloadable documents linked from the pages.

Note: An alternative to using a configuration file to crawl downloadable documents is to crawl the EPiServer CMS File Manager content (see "Configuring the EPiServer CMS Source to Crawl the File Manager" on page 932).
To create and use an EPiServer CMS configuration file

1. Using an administrator account, connect to the Coveo Master server.

2. Using a text editor:
   a. Create an XML file respecting the format illustrated in the following commented example.

```xml
<episerverdocumentconfig>
  <!- This is the type of item. For now, this config only applies for type "page" -->
  <page>
    <!- This is the type of pages, as defined within EPiServer -->
    <pagetype>
      <!- The value of pagetype -->
      <string>[AlloyTech] Document</string>
    </pagetype>
    <fieldstodownload>
      <!- this is the list of fields that the connector attempts to download as documents. -->
      <fieldnames>
        <!- This is the value of the metadata contained in the page that allows to retrieve the document. -->
        <string>DocumentInternalPath</string>
      </fieldnames>
    </fieldstodownload>
  </page>
</episerverdocumentconfig>
```

b. Save the file using a name of your choice in the [Index_Path]\Config folder.

Example: C:\CES7\Config\MyEPiServerCMSConfig.xml

3. To instruct the source to use this configuration file, add the ConfigFile hidden parameter to the EPiServer CMS source and use the filename and path where you saved the file as the value for the parameter (see "Modifying Hidden EPiServer CMS Source Parameters" on page 936).


The Coveo connector for EPiServer CMS system uses a built-in mapping to determine what metadata from your original documents are associated with fields for the documents in the Coveo index. The content of the built-in mapping file is presented below.

```xml
<?xml version="1.0" encoding="utf-8" ?>
<EpiServerMapping>
  <Mapping type="Default">
    <Fields>
      <Title>%[coveo_Title]</Title>
      <ModifiedDateUtc>%[coveo_DateModified]<br />ModifiedDateUtc)</ModifiedDateUtc>
      <CustomFields>
        <CustomField name="sysauthor"><%[coveo_CreatedBy]</CustomField>
      </CustomFields>
    </Fields>
  </Mapping>
  <Mapping type="Page">
    <Fields>
      <ClickableUri>%[coveo_ServerUrl]%[coveo_StaticLinkUrl]</ClickableUri>
      <PrintableUri>%[coveo_ServerUrl]%[coveo_StaticLinkUrl]</PrintableUri>
    </Fields>
  </Mapping>
</EpiServerMapping>
```
You can optionally create and use a custom mapping file to tailor the mapping to your needs.

To create and use a custom EPiServer CMS mapping file

1. Using an administrator account, connect to the Coveo Master server.

2. Using a text editor:

   a. Create an XML file respecting the format illustrated in the following commented example.

```
<?xml version="1.0" encoding="utf-8" ?>
<EpiServerMapping>
  <!-- These fields will be applied to all the documents that have the mappings defined later. -->
  <CommonMapping>
    <Fields>
      <Title>%[coveo_Title]</Title>
      <ModifiedDateUtc>%[coveo_DateModified]</ModifiedDateUtc>
      <CustomFields>
        <CustomField name="sysauthor">%[coveo_CreatedBy]</CustomField>
      </CustomFields>
    </Fields>
  </CommonMapping>
  <Mapping type="Default">
    <Fields>
      <Title>%[coveo_Title]</Title>
      <ModifiedDateUtc>%[coveo_DateModified]</ModifiedDateUtc>
      <CustomFields>
        <CustomField name="sysauthor">%[coveo_CreatedBy]</CustomField>
      </CustomFields>
    </Fields>
  </Mapping>
  <!-- It is valid to put the pagetype of an item to set metadata on. -->
  <Mapping type="[AlloyTech] News item">
    <Fields>
      <Title>Grosse Ventouse</Title>
      <ClickableUri>%[coveo_ServerUrl]%[coveo_StaticLinkUrl]</ClickableUri>
      <PrintableUri>%[coveo_ServerUrl]%[coveo_StaticLinkUrl]</PrintableUri>
      <Body>
        <html><body>
          %[MainBody]
          %[SecondaryBody]
          %[ThirdBody]
        </body></html>
      </Body>
      <CustomFields>
        <CustomField name="sysauthor">JoeBeton</CustomField>
        <CustomField name="pagetype">%[coveo_TypeName]</CustomField>
      </CustomFields>
    </Fields>
  </Mapping>
</EpiServerMapping>
```
b. Save the file using a name of your choice in the [Index_Path]\Config folder.

Example: C:\CES7\Config\MyEPiServerCMSMapping.xml

3. To instruct the connector to use this configuration file, add the MappingFile hidden parameter to the EPI Server CMS source and use the filename and path where you saved the file as the value for the parameter (see "Modifying Hidden EPI Server CMS Source Parameters" on page 936).

9.14.10 Modifying Hidden EPI Server CMS Source Parameters

The Add Source and Source: ... General pages of the Administration Tool present the parameters with which you can configure the connector for most setups. More advanced and more rarely used parameters are hidden. You can choose to make one or more of these parameters appear in the Add Source and Source: ... General pages of the Administration Tool so that you can change their default value.

Consider adding and setting values of hidden parameters only when they apply to one or more of your EPI Server CMS sources.

Hidden EPI Server CMS source parameters

ConfigFile (String)

This parameter is the full path to a custom EPI Server CMS configuration file (see "Creating and Using an EPI Server CMS Configuration File" on page 933).

MappingFile (String)

This parameter is the full path to a custom EPI Server CMS mapping file (see "Creating and Using an EPI Server CMS Mapping File" on page 934).
CMS Mapping File” on page 934).

**NumberOfRefreshThreads (Integer)**

This parameter is the number of refresh threads used by the source. The default value is 2.

**BatchSize (Integer)**

This parameter is the number of items to fetch per request made to the EPiServer CMS server. The default value is 50. The minimum value is 1. A small value forces the connector to make small but frequent queries to the server. A larger value leads to larger and less frequent queries.

**FileManagerConfigurationString (String)**

This parameter specifies the EPiServer File Manager content to crawl. The string is made up of the starting addresses to crawl separated by a semicolon character. Each starting address is composed of the values for the virtual path provider Name and VirtualPath attributes (see "Configuring the EPiServer CMS Source to Crawl the File Manager" on page 932).

**ShortCutTypesToIgnore (String)**

This parameter determines one or more types of content that the connector ignores to prevent indexing content more than once. The possible values are:

- 0 is a normal page.
- 1 is a shortcut to another page.
- 2 is an external link.
- 3 is only text instead of the page.
- 4 is a fetched data from another page.

The string is composed of one or more values separated by a semicolon character. The default value is 1;2;3.

**WebServiceUrl (String)**

This is the full URL to point to the Coveo Web service deployed on the EPiServer CMS installation. The default value is [StartingAddress]/WebServices/CoveoService.asmx (see "Configuring the Coveo Web Service on an EPiServer CMS Server" on page 926).

**IgnoreDeletedPages (boolean)**

Whether to ignore pages that were deleted (Recycle Bin). The default value is False. This parameter is available with CES 7.0.4887+

To modify hidden source parameters

**Note:** Use the following procedure only when you want to modify one or more of the above hidden source parameters.

1. Refer to "Adding an Explicit Connector Parameter" on page 450 to add a hidden source parameter.
2. For a new EPiServer CMS source, access the Add Source page of the Administration Tool to modify the value
of the newly added advanced parameter:
   a. Select Index > Sources and Collections.
   b. Under Collections, select the collection in which you want to add the source.
   c. Under Sources, click Add.
   d. In the Add Source page, edit the newly added advanced parameter value.

3. For an existing EPiServer CMS source, access the Source: ... General page of the Administration Tool to modify the value of the newly added advanced parameter:
   a. Select Index > Sources and Collections.
   b. Under Collections, select the collection containing the source you want to modify.
   c. Under Sources, click the existing source in which you want to modify the newly added advanced parameter.
   d. In the Source: ... General page, edit the newly added advanced parameter value, and then click Apply Changes.

9.15 File Connector

The Coveo connector for file shares allows you to index the content of files stored on local or network drives. The content of the files is integrated into the Coveo unified index, making the files easily searchable by end-users.

The File connector features are:

**Supported file shares**

The File connector can index files on file shares of the following types:

- Microsoft Windows Server (2012) and Microsoft Windows (8/7)
- Microsoft Windows Distributed File System (DFS)
- File share on other operating systems (ex.: UNIX, Linux, Mac) accessible through the Windows network.
  
  Paths and filenames must be compliant with the Windows naming conventions (see Naming Conventions).

**Note:** CES 7.0.7183+ (November 2014) The File connector supports long Unicode file paths up to 32,767 characters for both refresh and live monitoring operations, breaking the original 260 character maximum path length.

**Security**

The permissions associated with a file in the Coveo unified index are the same as the ones found in the file system.

**Identity impersonation**

You can configure each connector source to impersonate a different identity allowing to index several repositories that require different access credentials.
Incremental refresh

The File connector uses file live monitoring to identify modifications of indexed files. When this feature is enabled, CES processes modifications as soon as they are detected, thus keeping the unified index synchronized with the file system without requiring a source refresh.

Mail archives

You can optionally configure the File connector to open Microsoft Exchange Personal Folders (.pst) files and index the content of individual emails so that they become easily searchable by end-users. The File connector supports the Unicode and the legacy ANSI format of PST files (see "Mail Archive Indexing with the File Connector" on page 949).

Note: Microsoft Exchange Personal Folders (.pst) files are referred to as mail archives in the File connector documentation.

Note: The File connector is completely independent from the Desktop connector. While both connectors can crawl local and network drives, the File connector is configured by the Coveo administrator and the crawling process runs on the Coveo server. The Desktop connector is configured by end-users using the Desktop Integration Package (DIP) and the crawling process runs on their computers. Both connectors send content to the unified index on the Coveo server.

Connector Feature History

<table>
<thead>
<tr>
<th>CES version</th>
<th>Monthly release</th>
<th>Features</th>
</tr>
</thead>
<tbody>
<tr>
<td>7.0.7183</td>
<td>November 2014</td>
<td>Support for long file paths [more]</td>
</tr>
<tr>
<td>7.0.5425</td>
<td>May 2013</td>
<td>Support of permission levels and sets</td>
</tr>
</tbody>
</table>

9.15.1 File Connector Deployment Overview

The following procedure outlines the steps needed to bring content from file shares into the Coveo unified index using the File connector. The steps indicate the order in which you must perform configuration tasks.

1. Validate that your environment meets the requirements (see "File Connector Requirements" on page 940).

2. Determine how you will organize your File connector sources and collections within the Coveo unified index (see "Planning Your File Connector Collections and Sources" on page 940).

3. Select or create one or more necessary crawling accounts for the file share.

   The File connector needs an account with which it can crawl the complete content (see "Setting up a File System Crawling Account" on page 942).

4. Optionally, configure the File connector to index Microsoft Exchange mail archives.

   The File connector needs specific configuration to be able to open PST files and efficiently index their content (see "Mail Archive Indexing with the File Connector" on page 949).
5. In the Coveo Administration Tool, for each planned source:
   a. Optionally, configure the user identity.
      
      By default the File connector crawls the file share with the CES service identity. It is generally better to rather select or create a file share account with appropriate permissions to be used by the connector to crawl the file share (see "Setting up a File System Crawling Account" on page 942). You will then assign this crawling account to a user identity in the domain\username form (see "Adding a User Identity" on page 420), and assign the user identity to the source (see "Configuring and Indexing a File Connector Source" on page 942).
   
   b. Configure and index the File connector source.
      
      The File connector must know details about the file shares to be able to index their content (see "Configuring and Indexing a File Connector Source" on page 942).

6. In the Interface Editor, ensure that the collections containing the new File connector sources are included in the scope of the appropriate search interfaces.

7. Verify that the target content is available from the appropriate search interfaces.

8. Optionally, modify hidden source parameters

   Once your File connector source is up and running, if you encounter specific issues, consider modifying some hidden source parameters to resolve the issues (see "Troubleshooting File Connector Issues" on page 961 and "Modifying Hidden File Connector Source Parameters" on page 948).

9.15.2 File Connector Requirements

Your environment must meet the following requirements to be able to use the File connector:

- Coveo license for the File Connector

  Your Coveo license must include support for the File Connector to be able to use this connector.

- When indexing PST mail archives, Microsoft MAPI component on the Coveo server

  The File connector needs the Microsoft MAPI component to open PST files (see "Installing the Microsoft MAPI Component for Mail Archive Indexing" on page 951).

- When the access to communication ports between the Coveo Master server and the file share server(s) is restricted, the appropriate ports must be opened in the network infrastructure such as in firewalls (see Understanding Shared Folders and the Windows Firewall).

9.15.3 Planning Your File Connector Collections and Sources

The content of the Coveo unified index is organized in collections and each collection contains one or more sources. Before starting to deploy the File connector, you should determine how to organize collections and sources for the content of your file shares.
Consider the following facts:

- End-users can see collections names in search interface elements, while sources are generally only visible by Coveo administrator in the Administration Tool.

  **Note:** The source names can appear in the search interface for example when a custom facet presents `@syssource` elements.

- You can configure a search interface to include a **Collection** facet or collection check boxes below the search box so that end-users can refine search results based on collections.

- Each search interface has a specific scope that is defined by including one or more collections in which to search.

- When you create a collection, you can set permissions on the collection by specifying users or groups allowed to search the content of the collection.

- Similarly, when you create a source, you can set permissions on the source by specifying users or groups allowed to search the content of the source.

Consider the following recommendations when planning collections:

- Separate your file share content in collections that are meaningful to end-users and that are useful to refine results.

  **Example:** When you have network file servers for different locations in your organization, create a collection for each file server:
  - New York file share
  - San Francisco file share
  - Houston file share

- When creating a collection, choose a name that is clear and meaningful to end-users.

- Consider creating separate collections for separate audiences when you define specific search interfaces for specific audiences.

Consider the following recommendations when planning sources:

- Create separate sources when you need different impersonators to fully crawl different file shares or file share sections.

- When you choose to index mail archive (.pst) files, create a source to exclusively crawl mail archive files and exclude mail archive files from the source that crawls all other file types within the same file share.

- Consider creating separate sources when you want to set different permissions to different sections of a file share.

- Avoid grouping local and remote servers on the same source to prevent delaying source refresh on all servers when one server stops responding.
9.15.4 Setting up a File System Crawling Account

The File connector needs to connect to the file system using an account that has read access to all the content that you want to bring into the Coveo unified index.

By default, the File connector crawls the file share with the CES service identity. You can also select or create a file share account with appropriate permissions to be used by the connector to crawl the file share. This is typically done in Active Directory by creating an account that has full read permissions throughout the file shares to index. A best practice is to create a dedicated account for this purpose with a strong password that never changes.

In CES, you will assign this account to a user identity (see "Adding a User Identity" on page 420), and you will assign the user identity to a source (see "Configuring and Indexing a File Connector Source" on page 942).

**Important:** When indexing PST mail archive files, the crawling account must also have write and modify permissions. When the mail archive files are stored in a given folder, you can set up the account so it only has write access to that folder; however, when the mail archive files are scattered through different locations, give the account write access to the entire repository being indexed.

When you want or need to use different accounts for various files shares or file shares sections, consider creating two or more sources and assign a different user identity to each source.

**Example:** You can index the complete content of a file share except mail archive files with one source using an account with full read permissions and use a second source pointing to the folders containing PST files and use an account with read and write permissions to index only the content of PST files.

9.15.5 Configuring and Indexing a File Connector Source

A source defines a set of configuration parameters for one or more file shares or file share sections.

**Note:** Create two or more sources when file shares or file share sections need different parameters sets. A source uses one or more starting addresses to determine locations to crawl and index.

To configure and index a File connector source

1. On the Coveo server, access the Administration Tool.
2. Select Index > Sources and Collections.
3. In the Collections section:
   a. Select an existing collection in which you want to add the new source.
      OR
   b. Click Add to create a new collection.
4. In the Sources section, click Add.
   The Add Source page that appears is organized in three sections.
5. In the **General Settings** section of the **Add Source** page:

![Add Source Page](image)

a. Enter the appropriate value for the following required parameters:

**Name**

Enter a descriptive name of your choice for the connector source.

**Example:** Corporate network file share

**Source Type**

Select the connector used by this source. In this case, select **Files**.

**Addresses**

The list of starting address URIs indicating locations to index, one entry per line. You can specify the URIs as local or network paths. Addresses can represent a file system folder or file, a mail archive, or even a folder within a mail archive.
Examples:

Network folder: file://svr-fileshare/root
Local folder: file:///c:/fileshare/root/
Local file: file:///c:/fileshare/root/docs/work.doc
Mail archive: file://svr-fileshare/mails/jsmith.pst
Folder in a mail archive: file://svr-fileshare/mails/jsmith.pst/work
IP address file://192.168.1.2/share

Important: When you use paths containing drive letters as starting addresses (ex.: C:\fileshare), users will not be able to open the resulting links in the search result page. A better practice is therefore to rather index network file shares (ex.: \Intranet\fileshare).

Refresh Schedule

Time interval at which the source is automatically refreshed to keep the index content up-to-date. The recommended Every day option instructs CES to refresh the source everyday at 12 AM.

Note: You can create new or modify existing source refresh schedules.

b. Review the value for the following parameters that often do not need to be modified:

Rating

Change this value only when you want to globally change the ranking associated with all items in this source relative to the rating of other sources.

Example: If this source was for a legacy system, you may want to set this parameter to Low, so that in the search interface, results from this source appear later in the list compared to those from other sources.

Document Types

If you created a custom document type set for this source, select it. Otherwise, select Default.

Active Languages

If you defined custom active language sets, ensure to select the most appropriate for this source.

Fields

If you defined custom field sets, ensure to select the most appropriate for this source.

6. In the Specific Connector Parameters & Options section of the Add Source page:
a. Enter the appropriate value for the following parameters when you optionally want to index the content of mail archive files:

**Mapping Archives Configuration File**

When you decide to use a mail archive mapping file, enter the absolute full path pointing to your mapping file (see "Mail Archive Indexing with the File Connector" on page 949 and "Creating a Mail Archive Mapping File" on page 959).

**Example:** `C:\CES\Config\Coveo.CES.CustomCrawlers.File.MailArchives.config`

**Expand Mail Archives**

Select to index the content of mail archives (.pst). The default is false.

b. The default values for the following parameters generally do not need to be changed:

**Number of Live Monitoring Threads**

Determines the number of file system changes that the connector live monitoring can process simultaneously. The default and recommended value is 1.

**Max Number of Retries**

Number of retries to perform when indexing fails for a file that is opened by another application. The default and recommended value is 2.

**Number of Refresh Threads**

Determines the number of files that the connector can refresh simultaneously. The default and recommended value is 2.
Expand Before Filtering

By default this option is not selected so that the crawler applies inclusion and exclusion filters on files but also on folders before crawling so that it only expands folders that you want to index. In rare cases where an inclusion or exclusion filter should only be applied to files (ex. *.tif), you need to select this option so that the crawler fully expands folders to see all files and effectively applies the filters.

**Note:** Selecting this option can have a significant performance cost. The best practice is to use inclusion or exclusion filters to specify folders, not file types. Rather use document type sets to specify the file types to be indexed.

Index Share Permissions

By default this option is cleared. Select this option to index both the share and NTFS permissions (see the Microsoft document Share and NTFS Permissions on a File Server).

Parameters

Click Add Parameter when you want to show advanced hidden source parameters (see "Modifying Hidden File Connector Source Parameters" on page 948).

c. The **Option** check boxes generally do not need to be changed:

Index Subfolders

Check to index all subfolders below the specified starting addresses.

**Note:** You can control more precisely specific folders or files to crawl using inclusion or exclusion filters.

Index the document’s metadata

When selected, CES indexes all the document metadata, even metadata that are not associated with a field. The orphan metadata are added to the body of the document so that they can be searched using free text queries.

When cleared (default), only the values of system and custom fields that have the **Free Text Queries** attribute selected will be searchable without using a field query.

**Example:** A document has two metadata:

- LastEditedBy **containing** the value Hector Smith
- Department **containing** the value RH

In CES, the custom field CorpDepartment is bound to the metadata Department and its **Free Text Queries** attribute is selected.

When the **Index the document's metadata** option is cleared, searching for RH returns the document because a field is indexing this value. Searching for hector does not return the document because no field is indexing this value.

When the **Index the document's metadata** option is selected, searching for hector also returns the document because CES indexed orphan metadata.
Document's addresses are case-sensitive

Leave the check box cleared. This parameter needs to be checked only in rare cases for case sensitive systems in which distinct documents may have the same file name but with different casing.

Generate a cached HTML version of indexed documents

When you select this check box (recommended), at indexing time CES creates HTML versions of indexed documents and saves them in the unified index. In the search interfaces, users can then more rapidly review the content by clicking the Quick View link to open the HTML version of the item rather than opening the original document with the original application.

When the source includes mail archives files, you must select this option to ensure users can view the content of mail archives items.

Consider clearing this check box only if you do not want to use Quick View links or to save resources when building the source.

Open results with cached version

Leave this check box cleared (recommended) so that in the search interfaces, the main search result link opens the original document with the original application. Consider selecting this check box only when you do not want users to be able to open the original document but only see the HTML version of the document as a Quick View. When this option is selected, you must also select the Generate a cached HTML version of indexed documents check box.

Note: When you index mail archive files, a custom document type set handles how mail archive items are opened from the search interfaces (see "Setting up a Document Type for Mail Archive Indexing" on page 958).

7. In the Security section of the Add Source page:

   a. In the Security Provider drop-down list, select Active Directory or a custom Active Directory security provider that you created for a specific domain.

   b. In the Authentication drop-down list, when you chose to use a specific account to crawl the file system (see "Setting up a File System Crawling Account" on page 942), select the user identity that you created for this account. Leave this parameter empty when you want the connector to crawl the file system using the

www.coveo.com
CES service identity.

c. Click **Save and Start** to save the source configuration and start indexing this source.

8. Validate that the source building process is executed without errors:

   - In the navigation panel on the left, click **Status**, and then validate that the indexing proceeds without errors.
   
   OR

   - Open the CES Console to monitor the source building activities.

9.15.5.1 Modifying Hidden File Connector Source Parameters

The **Add Source** and **Source: ... General** pages of the Administration Tool present the parameters with which you can configure the connector for most file share setups. More advanced and more rarely used parameters are available but hidden. You can choose to make one or more of these parameters appear in the **Add Source** and **Source: ... General** pages of the Administration Tool so that you can change their default value. Consider changing values of hidden parameters only when you encounter time out error messages or performance issues.

The following list describes the available advanced hidden parameters for File connector sources. The parameter type (integer, string,...) appears between parentheses following the parameter name.

**EnableCrawlDFSReferralLink (Boolean)**

Set to True to enable crawling of Distributed File System (DFS) referral links. This option is useful when Windows perceives the crawling by the connector as a Denial-of-Service attack (see "Access denied when crawling through a Distributed File System (DFS)" on page 961). The default value is **False**.

**IgnoreUnresolvedDeniedSecurities (Boolean)**

Set to True to ignore unresolved denied permissions. This option is useful to voluntarily ignore unresolved denied security errors. The default value is **False**.

**Example:** When a user or group no longer exists, accessing their documents is denied and causes unresolved security exceptions with a message like: *Unexpected error occurred while retrieving content from directory. - Access to the path [path] is denied.*

**Important:** Enable this parameter with caution as it can create a security hole.

**LiveMonitoringEventsQueueMaxSize (Integer)**

Maximum number of modification events to store for each monitored starting address before discarding them. Discarded modification events will be indexed the next time the source is refreshed. This parameter is useful to prevent queuing a large number of modification events that would take a large amount of memory on the server when many files under the starting address are modified in a very short period of time. The default value is 100,000.

**RetryDelay (Integer)**

Delay (in seconds) before retrying to process a document that failed to be indexed. The default value is 30. Consider increasing the value when you think that this can increase chances for the file to be available for
crawling.

**RetryQueueMaxSize (Integer)**

Maximum number of items to store in the retry queue before discarding them. The default value is 100. Consider increasing the value when you experience frequent sharing violation when crawling and want to ensure no document is discarded (see “Some items are not added to the retry queue when they failed to be indexed” on page 962).

**TempFileRegex (String)**

Regular expression (regex) used to exclude unwanted temporary files from indexation. By default this parameter is empty. This option is useful when exclusion filters are not precise enough to exclude specific files such as temporary files. The option can also be used to filter other types of files using a custom regular expression.

**FileSystemWatcherBufferSize (Integer)**

Buffer size of the File System Watcher instance used by the File Crawler to monitor file system events. For best performance, use a multiple of 4 KB (4096). Increasing this buffer size is expensive because it comes from non-paged memory that cannot be swapped out to disk. Keep the buffer as small as possible. The default value is 8192.

Use the following procedure only when you want to modify one or more of the above hidden source parameters.

To modify hidden File connector source parameters

1. Add one or more hidden source parameters (see "Adding an Explicit Connector Parameter" on page 450).
2. For a new File source, access the Add Source page of the Administration Tool to modify the value of the newly added advanced parameter:
   a. Select Index > Sources and Collections.
   b. Under Collections, select the collection in which you want to add the source.
   c. Under Sources, click Add.
   d. In the Add Source page, edit the newly added advanced parameter value.
3. For an existing File source, access the Source: ... General page of the Administration Tool to modify the value of the newly added advanced parameter:
   a. Select Index > Sources and Collections.
   b. Under Collections, select the collection containing the source you want to modify.
   c. Under Sources, click the existing File connector source in which you want to modify the newly added advanced parameter.
   d. In the Source: ... General page, edit the newly added advanced parameter value.

9.15.6 Mail Archive Indexing with the File Connector

The File connector can index Microsoft Exchange mail archive files (.pst) that reside on crawled file shares. The File connector supports the legacy ANSI PST file format that was used up to Microsoft Outlook 2003 as well as the
Unicode format that was introduced in Microsoft Outlook 2003 and is the only format used since Microsoft Outlook 2007.

Indexing PST mail archive files requires some specific configuration. Consequently, a best practice is to create and configure one source that exclusively index mail archive files on a file share (see "File Connector Mail Archive Indexing Deployment Overview" on page 951).

**Note:** You can also deploy the Desktop Integration Package (DIP) together with the Desktop connector. End-users can then configure the DIP to crawl mail archive files stored on the local hard drives on their computer or on private network folders so that their content is searchable from the unified index on the Coveo server.

### 9.15.6.1 About Permissions

The following list describes how the File connector manages permissions on items retrieved from mail archive files:

1. **Mailbox**

   When you use an optional mail archive mapping file, you can associate a specific mailbox to a specific mail archive. The permissions associated to the mailbox in Active Directory are assigned to the mail archive. This type of permission is used first when it exists (see "Creating a Mail Archive Mapping File" on page 959).

   **Example:** For a mail archive file containing emails of one user, you can associate the mailbox of the specific user to the mail archive file.

2. **Mapping file security**

   When you use an optional mail archive mapping file, you can define allowed users (*AllowedUser*) in the CommonMappings and Mapping sections of the mapping file for a specific mail archive file. This type of permission is added to the mailbox permissions (see "Creating a Mail Archive Mapping File" on page 959).

   **Example:** For a mail archive file containing shared emails from the support department, you can allow all users working in the support department to be able to search items from this file.

3. **File system**

   When the permissions of a mail archives file is not defined in a mapping file, the File connector uses the NTFS permissions for the mail archive file to set the permissions on each mail archive item in the unified index.

### 9.15.6.2 Live Monitoring Limitation

The File connector cannot index mail archives that are currently opened in a Microsoft Outlook profile. Microsoft Outlook always opens a mail archive in exclusivity mode. Any File connector attempt to open mail archives file during that time fails. Consequently, it is not possible to effectively implement live monitoring on mail archives. Consider turning off live monitoring on the source created to index your mail archives (see "Toggling Live Monitoring for a Source" on page 282).

It is recommended to only index repositories containing mail archives that are not used and to schedule periodic refresh schedules to pick up any changes that could be made to the archives.
9.15.6.3 About the Mail Archives Modified Date Attribute

The File connector needs to first add the mail archive to a temporary Microsoft Outlook profile to be able to make MAPI calls to open and process the archive content. Unfortunately, this operation causes Microsoft Outlook to update the modified date attribute of the mail archive file to the current date and time. When the indexing of the mail archive file is completed, the File connector sets the modified date attribute back to its original value. Consequently, for the time required to process the mail archive file, the modified date is changed to the current one.

**Important:** A temporary change of the modified date attribute for mail archive files could have consequences when a backup or archiving software actively monitors the repository to detect changes to files based on the modified date attribute.

9.15.6.4 File Connector Mail Archive Indexing Deployment Overview

When you choose to index the content of mail archive files using the File connector, you need to perform the following tasks.

1. **Install the Microsoft MAPI component.**
   
   The File connector uses the Microsoft MAPI component to access the content of mail archive files. This component must be installed on the Coveo Master server (see "Installing the Microsoft MAPI Component for Mail Archive Indexing" on page 951).

2. **Create a custom document type set.**
   
   In the search results, the URI of archived email results cannot be opened in the original mail application. The solution is to use the Quick View to open a cached HTML version created in the unified index when the item was crawled. You need to create a special document type set to do so (see "Setting up a Document Type for Mail Archive Indexing" on page 958).

3. **Consider creating an optional mapping file.**
   
   By default, the file crawler uses the NTFS permissions on the mail archive file to set the permissions for each mail archive item in the unified index. You need to create and use a mail archive mapping file when you want to override these permissions, index password protected mail archive files, or make mail archive items appear in email search interfaces (see "Creating a Mail Archive Mapping File" on page 959).

4. **Ensure the File connector runs in a 32-bit process.**
   
   On a 64-bit server, the File connector must run in a 32-bit process to be able to index PST mail archives. This is the default configuration because the connector uses a third-party library that does not support 64-bit processes. The parameter for the connector process type (32-bit or 64-bit) affects all sources for this connector. Consequently, you must ensure that the File connector runs in a 32-bit process (see "Selecting a 32-bit or 64-bit Process for a Connector" on page 454).

9.15.6.5 Installing the Microsoft MAPI Component for Mail Archive Indexing

The File connector uses the Microsoft Messaging API (MAPI) client libraries to access mail archive content. You therefore need to install this Microsoft component on the Coveo server when you want to index mail archive content.
You must install the MAPI component using the Microsoft Office installer on the Coveo server. You can install only the MAPI component using the installation options.

**Note:** Do not use the Microsoft standalone installation package for MAPI and CDO. This package does not install all the components that the File connector needs.

You can use the installer for various versions of Microsoft Office:

- "Installing the MAPI components with Microsoft Office 2010" on page 952
- "Installing the MAPI components with Microsoft Office 2007" on page 954
- "Installing the MAPI components with Microsoft Office 2003" on page 956

Installing the MAPI components with Microsoft Office 2010

1. Using an administrator account, connect the Coveo Master server on which a File connector needs to access mail archive content.

   **Note:** By default, the Microsoft Office Professional Plus 2010 installer does not offer options to select specific components to install. You can however use the Office Customization Tool that is part of the setup program to specify components to install.

2. Launch the Microsoft Office 2010 installer using the /admin option to start the Office Customization Tool:
   a. Open a **Command Prompt** window.
   b. Type `setup.exe /admin` at the command line from the root of the network installation point that contains the Office 2010 source files.

   **Example:** `\server\share\Office14\setup.exe /admin`

   The Office Customization Tool starts.

3. In the **Select Product** dialog box that appears:
   a. Select **Create a new Setup customization file for the following product**.
   b. Ensure Microsoft Office is selected in the **Product** list.
   c. Click **OK**.

4. In the **Microsoft Office Customization Tool**:
a. In the navigation panel on the left, under **Features**, select **Set feature installation states**.

b. In the central panel, expand the product tree to show **Microsoft Office > Microsoft Outlook > Outlook Messaging Components**.

c. Right-click **Outlook Messaging Components**, and then select **Run from My Computer**.

d. For all other product tree elements, right-click the element and then select **Not Available**.

e. On the menu, select **File > Save As** to save a customization .msp file with a name and to a location of your choice.

**Example:** C:\user\username\Desktop\MyMSOfficeConfig.msp

5. Start the Microsoft office installer using the setup command-line option /adminfile to specify the fully-qualified path of the location of the .msp file:

   - In a **Command Prompt** window, type a command in the form:

     ```
     setup.exe /adminfile [path]\[customization_file]
     ```

   **Example:**

     ```
     setup.exe /adminfile C:\user\username\Desktop\MyMSOfficeConfig.msp
     ```

6. In the **Microsoft Office Professional Plus 2010** dialog box:

   a. Read and accept the Microsoft Software License Terms, and then click **Continue**.

   b. In the **Choose the installation you want** screen, click **Install Now** to install the components selected in the customization file.
The **Installation Progress** screen appears while the installation is performed.

c. In the **Complete your Office experience** screen, click **Close**.

### Installing the MAPI components with Microsoft Office 2007

1. Using an administrator account, connect the Coveo Master server on which a File connector needs to access mail archive content.

2. Launch the Microsoft Office 2007 installer.

3. Read and accept the Microsoft Software License Terms, and then click **Continue**.

4. In the **Choose the installation you want** screen, click **Customize**.
5. In the **Installation Options** tab:

   a. Expand the product tree to show **Microsoft Office > Microsoft Office Outlook > Outlook Messaging Components > Outlook Mapi Service Providers**.

   b. Click **Outlook Mapi Service Providers**, and then select **Run from My Computer**.

   c. For all other product tree elements, click the element and then select **Not Available**.
d. Click **Install Now**.

   The **Installation Progress** screen appears while the installation is performed.

6. In the last screen, click **Close**.

Installing the MAPI components with Microsoft Office 2003

1. Using an administrator account, connect the Coveo Master server on which a File connector needs to access mail archive content.


3. In the **User Information** screen, you can leave all parameters empty, and then click **Next**.

4. In the **Type of Installation** screen, select the **Custom Install** option, and then click **Next**.
5. In the **Custom Setup** screen:
   a. Unselect all applications except **Outlook**.
   b. Select the **Choose advanced customization of applications** check box, and then click **Next**.

6. In the **Advanced Customization** screen:
a. Set all installation options to Not available for applications other than Microsoft Office Outlook.

b. Under Microsoft Office Outlook, set Outlook Messaging Components to Run from my computer.

c. Click Next.

7. In the Summary screen, click Install.

9.15.6.6 Setting up a Document Type for Mail Archive Indexing

In the search results, the URI of an archived item result cannot be opened in the original mail application. The solution is to use the Quick View to open an HTML cached version of the content created in the unified index when the item was crawled. You need to create a special document type set for mail archives that instructs CES to open results with the HTML cached version.

**Note:** You need to verify that the Generate a cached HTML version of indexed documents option is selected for the source to ensure that a Quick View version of the mail archives items is created when CES crawls the source (see “Configuring and Indexing a File Connector Source” on page 942).

To set up a document type set for mail archives indexing

1. On the Coveo server, access the Administration Tool.

2. In the Administration Tool, select Configuration > Document Types.

3. In the Document Type Sets page, click Add.

4. In the Add Document Type Set page:
a. In **Name**, enter a name representing the document type set:

   **Example:** QuickViewMailArchives

b. In **Description**, optionally enter a description of the purpose of the document type set.

c. Click **Save**.

   The new document type set is displayed in the **Document Type Sets** list.

5. Click on the newly created document type set.

6. In the page that appears, in the **Name** list, click **Exchange Items**.

7. In the page that appears, in the **Option** section, select the **Open results with cached version** check box.

8. Click **Apply Changes**.

   **Important:** Ensure that every source used to index mail archives uses this new document type set (see "Configuring and Indexing a File Connector Source" on page 942).

### 9.15.6.7 Creating a Mail Archive Mapping File

The File connector can use a mail archive mapping file to get detailed instructions on how to open and index the content of mail archive files. Using a mail archive mapping file is not mandatory, and if you do, having a mapping file entry for each mail archive is not mandatory.

Associating a mail archive mapping file to a File connector source provides the following advantages:

- Allows indexing of password protected mail archive files.
- Allows to associate a Microsoft Exchange mailbox with a mail archive file so that the items it contains are indexed with the permissions associated with the mailbox. This also sets the sysmailbox field for the mail archive items, allowing the items to appear in email search interfaces.
- Can explicitly specify the permissions to the content of a mail archive file or to the content of a folder in a file by setting allowed users or groups.

To create a mail archive mapping file

1. Connect to the Coveo Master server using an administrator account.

2. Using a text editor, create an XML mapping file that respects the mail archive mapping file format and that describes the mail archive file that you want to index from a given source (see "Mail archive mapping file format" on page 959).

   **Tip:** You can start with the sample mail archive mapping file available in the [CES_Path]\Bin\Coveo.CES.CustomCrawlers.File.MailArchives.zip file on the Coveo server.

3. Save the mapping file on the Coveo master server with a name of your choice (ex.: NetworkShareMailArchivesMappingFile.config). The **recommended folder** is [Index_Path]\Config.

### 9.15.6.7.1 Mail archive mapping file format

The mail archive mapping file can be divided into two sections:
CommonMapping

Settings that apply to all mail archives, whether they are defined in the mapping file or not.

Mapping

Settings for a specific mail archive. A specific mapping overrides a mapping defined in the CommonMapping section.

The following sample of a mail archive mapping file illustrates how it can be organized and how to use the various XML elements.

```xml
<?xml version="1.0" encoding="utf-8" ?>
<MailArchives>
  <CommonMapping>
    <AllowedUsers>
      <AllowedUser type="Windows" allowed="true">
        <Name>corp\administrators</Name>
        <Server></Server>
      </AllowedUser>
      <AllowedUser></AllowedUser>
      <AllowedUsers></AllowedUsers>
    </CommonMapping>
    <Mapping type="\svr-archives\mail\employees\jsmith.pst">
      <Fields>
        <Password>12345</Password>
      </Fields>
      <Mailbox active="true">
        <LDAPSearchRoot>LDAP://OU=companynameOU, DC=corp, DC=companyname, DC=com</LDAPSearchRoot>
        <Name>jsmith@corp.com</Name>
      </Mailbox>
    </Mapping>
    <Mapping type="\svr-archives\mail\employees\jdow.pst">
      <!-- Jane Dow mailbox does not exists anymore, set mailbox active attribute to false -->
      <Mailbox active="false">
        <Name>jdow@corp.com</Name>
      </Mailbox>
    </Mapping>
  </CommonMapping>
</MailArchives>
```

In a mail archives mapping file, you can use the following elements:

Fields

The only field that you can specify for mail archives is the Password field. Since a mail archive can be password protected by a user when it is created, this field holds the password used when attempting to open protected archives. If the password of a protected archive is not defined in the mapping file, the archive will not be opened; hence, not indexed.

**Important:** Special care must be taken when specifying a mail archive password. When you specify a password in the mapping file for a mail archive file that has currently no password, the Microsoft MAPI component opens the mail archive and permanently sets the specified password to the mail archive file.

Mailbox

This is where a Microsoft Exchange mailbox can be associated to a mail archive. This association enables mail archive items to appear in the results of email search interfaces. Without a mailbox association, mail archives items can only appear in the results of generic search interfaces such as the All Content search interface.

The Mailbox element requires the following information:
Active

When this attribute is set to true, the security for the mailbox is resolved from Active Directory and is set on each item retrieved from the mail archive. When set to false, it blindly associates the mailbox to the archive items without retrieving its security or validating that the mailbox exists in Active Directory.

Name

Element used to specify the name of the mailbox and set the sysmailbox field.

Example: jsmith@corp.com

LDAPSearchRoot

This optional element specifies to the connector where to start looking in Active Directory. When this parameter is not specified, the connector looks at the root of Active Directory, which can be extremely large. By specifying a value, you can refine the search and speed up the mapping process.

Example: To search only within the organizational unit (OU) companynameOU within the domain corp.companyname.com, enter: LDAP://OU=companynameOU, DC=corp, DC=companyname, DC=com.

AllowedUsers

Use this element to grant or deny access to the mail archive content. These security settings complement existing ones retrieved from Active Directory when an active mailbox is specified for the archive.

The AllowedUser element requires the following information:

Type

Attribute used to set the type of users specified in the name element. The two possible values are Windows and WindowsSid.

Name

Element used to specify the name of the Windows User or Group in the form domain\username (ex.: corp\administrators).

Server

Element used to specify the name of the local machine when referring to local users or groups. For domain users, you should leave this element empty.

9.15.7 Troubleshooting File Connector Issues

Access denied when crawling through a Distributed File System (DFS)

Possible cause

When the File connector performs a Rebuild or a Refresh operation through a DFS, depending on the number of threads used and the overall crawling speed, several connections can be opened simultaneously to the targeted server. In some instances where the number of connections grows to a large number, Microsoft Windows can see this as a Denial-of-Service attack on the server and start refusing to create new connections to that server. When this situation arises, the File connector logs will display Access Denied Errors for any
items located on that server. You can confirm this situation by monitoring Windows Event Viewer logs for Event ID 2027.

Possible solution

If you encounter this problem, you can change your source starting address so it targets one of the DFS active referral links instead of going through the DFS itself. This could help resolve the problem if the server experiencing the connection problem is the DFS server and not the file share server where the resource being crawled is located.

Example: Replace the DFS starting address `\DFSName\Rootname\Ressource` by `\ServerName\RessourceFileShare`.

The File connector also has the ability to automatically attempt to detect and crawl a DFS active referral link instead of going through the DFS. You can add the `EnableCrawlDFSReferralLink` hidden File connector source parameter and set it to True to enable this feature which is disabled by default (see "Modifying Hidden File Connector Source Parameters" on page 948).

Some items are not added to the retry queue when they failed to be indexed

Possible cause

The File connector automatically retries to index any item that failed to be indexed because it was opened by another application during the initial crawling (sharing violation). To keep the retry queue to a reasonable size, the default maximum number of items in the queue is set to 100. When the connector encounters frequent sharing violations, the limit may be exceeded.

Possible solution

If you experience frequent sharing violations when crawling, you can increase the default value of the `RetryQueueMaxSize` hidden File connector source parameter (see "Modifying Hidden File Connector Source Parameters" on page 948).

When crawling a Network Share, the "CGLSecurity::SecurityInvalidUserOrGroup: No mapping between account names and security IDs was done" error is displayed for every file

Possible cause

Even though the starting address provided is valid, an error occurred when attempting to resolve the permissions on files from that address. This problem can occur with some network configurations where CES can’t properly interpret the host from the supplied starting address.

Possible solution

If you are using the network share fully qualified name, try to use its shortened version.

When crawling a mail archive with the Expand Mail Archives source option enabled, the "Failed to open mail archive, it is in use and cannot be accessed. Make sure it is not still opened in Outlook." error message is returned

**Possible cause**

The File connector cannot index the content of a mail archive that is currently opened in Microsoft Outlook.

**Possible solution**

Close the Archive in Microsoft Outlook and retry. When you encounter this error even after closing the archive in Microsoft Outlook, restart Microsoft Outlook to ensure it releases all handles on the archive.

When crawling a mail archive with the Expand Mail Archives source option enabled, the "Failed to open mail archive, it is password protected. The password specified in the Mail Archives Mapping File for this archive is incorrect." error message is returned

**Possible cause**

This message indicates that a password for the archive was found in the mail archive mapping file but the password is incorrect. Passwords are case sensitive.

**Possible solution**

Ensure that you specify the passwords in the File connector mapping file with the same casing as when you open the archives in Microsoft Outlook (see "Creating a Mail Archive Mapping File" on page 959).

When crawling a mail archive with the Expand Mail Archives source option enabled the "Failed to open mail archive, it is password protected. You need to add this archive password to the Mail Archives Mapping File, please refer to the Connector documentation for further details." error message is returned

**Possible cause**

This means that there is no password specified for the protected archive in the mail archive mapping file

**Possible solution**

Ensure that you specify a password for each protected archive file in the mail archive mapping file (see "Creating a Mail Archive Mapping File" on page 959). If you did specify a password for the archive, ensure the mapping type for the archive was properly entered and that it contains the full path to the archive.

**Example:** `<Mapping type="\\svr-archives\mail\employees\jdow.pst">

9.16 Gmail for Work Connector

**CES 7.0.7711+ (June 2015)**

The Coveo connector for Gmail for Work allows Coveo administrators to index and integrate the Gmail mailboxes content of their users into the Coveo unified index. The connector indexes all items and the attached permissions from all Gmail domain users so that in the Coveo search interfaces, a user can easily find any but only content to which he has access in Gmail.
9.16.1 Connector Features Summary

<table>
<thead>
<tr>
<th>Features</th>
<th>Supported</th>
<th>Additional information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Gmail for Work version</td>
<td>Latest cloud version</td>
<td>Following available Gmail for Work releases</td>
</tr>
<tr>
<td>Searchable content types</td>
<td></td>
<td>Emails and attachments</td>
</tr>
<tr>
<td>Content update</td>
<td>Incremental refresh</td>
<td>Full refresh or rebuild needed to capture domain, primary email and email aliases changes.</td>
</tr>
<tr>
<td></td>
<td>Full refresh</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Rebuild</td>
<td></td>
</tr>
<tr>
<td>Document-level security</td>
<td></td>
<td>The Gmail delegation feature is not yet supported, meaning a user can only search the content of his mailbox even if he has access to other users mailbox in Gmail for Work.</td>
</tr>
</tbody>
</table>

9.16.2 Features

The Gmail for Work connector features are:

**Content indexing**

The connector can retrieve and index exclusively the following Gmail types of items:

- Emails
- Attachments

**Mostly supported security model**

The connector mostly supports the Gmail security model by associating each item with a primary email and its aliases. This means that, in Coveo search interfaces, a user searching Gmail content only sees the content of his mailbox.

**Note:** In some cases, a user can have access to other users mailbox, but the Gmail delegation feature is not yet supported.

**Incremental refresh**

Supports incremental refresh to periodically query Gmail for the latest changes on messages (addition, deletion, edition, label change), keeping the index content up-to-date.

**Note:** A source full refresh or rebuild is needed to capture domain, primary email and email aliases changes.
Multithreading

The connector can run multiple threads, which can improve performances considerably (see Modifying Hidden Gmail for Work Source Parameters).

Pause/Resume

When indexing Gmail for Work content, the connector can be paused and resumed.

What's Next?

Review the steps to deploy the Gmail connector (see "Gmail for Work Connector Deployment Overview" on page 965).

9.16.3 Gmail for Work Connector Deployment Overview

The following procedure outlines the steps needed to deploy the Gmail for Work connector. The steps indicate the order in which you must perform configuration tasks on both the Google and Coveo servers.

To deploy the Gmail for Work connector

1. Validate that your environment meets the requirements (see "Gmail for Work Connector Requirements" on page 966).

2. On the Google server:
   a. Create a Google API Console project to authorize the Coveo connector to access the Gmail mailboxes of your users (see "Authorizing the Coveo Connector to Access Your Users Gmail Mailboxes" on page 967).
   b. Modify security parameters in your Google Apps account to grant the connector access to the Google Apps (see "Authorizing the Coveo Connector to Access Your Google Apps for Work" on page 971).

3. On the Coveo server, in the Coveo Administration Tool:
   a. Create security providers:
      In Gmail, users are identified by their email addresses. Consequently, permissions returned by the connector for each document are email addresses (primary and aliases). The connector requires a security provider to uniquely identify users from their email addresses.
      You must thus create one or more security provider depending on how users are authenticated when they access the search interface:
      
      - When authenticated with an Active Directory account:

        **Note:** Mapping Gmail users to Microsoft AD users is possible when the email specified in the AD for your users is the same as their primary email or one of their email aliases in Gmail. Otherwise, you may require to use a third security provider (e.g., REGEX Transform Member Name) in between the Email and AD security providers to map member types. Contact Coveo Support for assistance.

        i. Create an Email security provider to be used to map AD users to their email (see "Configuring an Email Security Provider" on page 65).
ii. Create or configure an Active Directory security provider, and then map AD users to Email users by selecting the Email security provider you just created in the Email provider drop-down list (see "Configuring an Active Directory Security Provider" on page 1141).

**Notes:**
- CES comes with an Active Directory security provider that you can configure to connect to the default domain. When your environment contains more than one domain, you can select an Active Directory security provider that you created for other domains.
- When configuring the Gmail source, select the Email security provider.

- When authenticated with the same email as in Gmail, create an Email security provider for your users to be recognized by their email addresses (see "Configuring an Email Security Provider" on page 65).

b. Create a Gmail field set to take advantage of the available Gmail metadata.
   
i. It is recommended to start by importing the default Gmail field set file (\CES_Path\Bin\Coveo.CES.CustomCrawlers.Gmail.FieldSet.xml) to create fields for all the metadata available by default from Gmail documents.

ii. When you created custom metadata for your Gmail documents, add corresponding fields to the field set.

c. Configure and index a Gmail for Work source.
   
The connector must know details about the authorized access to the Gmail mailboxes of your users to index their content (see "Configuring and Indexing a Gmail for Work Source" on page 973).
   
d. If you encounter issues, verify if modifying the default value of hidden source parameters can help resolve the problems (see "Modifying Hidden Gmail for Work Source Parameters" on page 978).

9.16.4 Gmail for Work Connector Requirements

Your environment must meet the following requirements to be able to use the Gmail for Work connector:

- **CES 7.0.7711+ (June 2015)**

- Coveo license for the Gmail (Google Apps) connector

   Your Coveo license must include support for the Gmail for Work connector to be able to use this connector.

- A valid Google Account

   Using a Google Account with administrator privilege, you must log in the Google Developers Console to authorize Coveo to access the Gmail mailboxes of your users (see Authorizing the Coveo Connector to Access Your Users Gmail Mailboxes).

- Administrator credentials to your Google Apps for Work account

   You must log in to your Google Apps account to modify security options and authorize Coveo to access your Google Apps for Work (see Authorizing the Coveo Connector to Access Your Google Apps for Work).
What's Next?

Grant Coveo access to the Gmail mailboxes of your users by creating a Google API Console project and modifying security options in your Google Apps account (see "Authorizing the Coveo Connector to Access Your Users Gmail Mailboxes" on page 967 and "Authorizing the Coveo Connector to Access Your Google Apps for Work" on page 971).

9.16.5 Setting Google Permissions Gmail for Work Connector

Before you start configuring the Gmail for Work Coveo connector, you must first set appropriate Google permissions.

Refer to the following topics to perform the necessary Google security configuration:

1. "Authorizing the Coveo Connector to Access Your Users Gmail Mailboxes" on page 967
2. "Authorizing the Coveo Connector to Access Your Google Apps for Work" on page 971

9.16.5.1 Authorizing the Coveo Connector to Access Your Users Gmail Mailboxes

You must perform a G Suite domain-wide delegation of authority to authorize the Coveo connector to access the Gmail for Work content that you want to index.

To authorize the connector to access your users Gmail mailboxes

1. Go to the Google Developers Console, and log in using a Google Account with administrator credentials.

2. At the left of the Filter by name, ID or label input, click the drop-down menu, and then select the organization in which you want to create the Google Developer Console project.

3. Create an API project for the Coveo connector (CES 7) or source (Coveo Cloud):
   a. In the Manage resources panel, click Create a project.
   b. (When your project limit is exceeded) In the Increase Project Limit page, click Request increase, and then complete the form.
   c. In the New Project dialog page, enter the project required information.
i. Enter a Project name.

**Note:** The project ID is automatically created based on the project name. You can always modify the project ID by clicking Edit.

ii. (When you create the first project in your organization only) Answer the Please email me updates regarding feature announcements, performance suggestions, feedback surveys and special offers. question using the Yes or No checkbox.

iii. (When you create the first project in your organization only) After you have read and agree to the Google Play Android Developer API Terms of Service, click the Yes check box.

iv. Click Create.

4. Enable the required Google APIs.

   a. Access the API Library page by clicking Google APIs in the top menu.

   b. In the API Library page, enable the Gmail API and Admin SDK APIs:

      i. Under Google APIs, use the search box to search and select Gmail API or Admin SDK.

      ii. In the Gmail API or Admin SDK page, in the action bar, click Enable.

      iii. In the action bar, click the back button (←).

      iv. Repeat the procedure for the other API.

5. Create a service account project for the Coveo connector (CES 7) or source (Coveo Cloud).
a. Access the Service accounts page:
   i. At the top of the sidebar on the left, click the Product & services icon (≡).
   ii. In the sidebar on the left, hover IAM & Admin, and then click Service accounts.

b. In the Service Accounts page, in the action bar, click Create service account.

c. In the Create service account dialog box:
   i. If not already done, set a product name (e.g., Coveo Connector) that will appear on the consent screen by clicking Configure consent screen, providing the requested information, and then clicking Save.

      Note: The consent screen will appear when the application requests read access to the users' data.

   ii. Enter a Service account name.

      Example: Coveo Connector

   iii. (Optionally) Edit the Service account ID or generate another one by clicking the refresh icon 🔄.

      Note: The service account ID is automatically created based on the service account name.

   iv. Click the Role drop-down list menu, and then select Service account > Service account admin.

   v. Select the Furnish a new private key checkbox, and then under Key type, select the P12 checkbox.

   vi. Select the Enable G Suite Domain-wide Delegation checkbox.

   vii. Click Create.

      Note: A private key is automatically downloaded as a Personal Information Exchange (.p12) file in your browser download folder.

d. In the Service account created dialog box that appears, take note of the private key password, and then click Close.

6. (For CES 7 customers only) Using an administrator account, connect to your Coveo Master server, and then copy the downloaded private key [GUID]-privatekey.p12 file to a folder accessible to Coveo Enterprise Search, typically in the [Index_Path]\Config folder.

7. Back in the Service Accounts page, on the service account row you just created, in the Options column, click View Client ID.

8. In the Client ID Service account client page, take note of the following information that you will need later when configuring your Gmail for Work source:
   - Client ID
   - Email address (under the Service account name)
9. Ensure the Gmail API request limit is high enough to reduce throttling errors (GMAIL_THROTTLING_ERROR).

   a. Access the Gmail API page:
      i. In the top menu, click Google APIs.
      ii. In the Dashboard page, in the enabled APIs table, click Gmail API.

   b. In the Gmail API page, select the Quotas tab.

   c. In the Quotas tab, ensure the Queries per 100 seconds per user limit is a high number such as 25,000.
queries.

What's Next?

You must modify security parameters in your Google Apps account to grant the connector (CES 7) or source (Coveo Cloud) access to your Google Apps for Work (see "Authorizing the Coveo Connector to Access Your Google Apps for Work" on page 971).

9.16.5.2 Authorizing the Coveo Connector to Access Your Google Apps for Work

You must perform a Google Suite domain-wide delegation of authority to authorize the Coveo connector (CES 7) or source (Coveo Cloud) to access your Google Apps for Work.

To authorize the connector to access your Google Apps for Work

1. Go to your Google Apps for Work domain Admin console:
   a. Access the User hub with an administrator account.
   b. In the hub, click Admin Console.
2. In the Google Admin Console, click Apps.
3. In the Apps page, select G Suite.

4. In the G Suite page, ensure that for Gmail, the Status is set to On for everyone.

5. Grant access to users data for the Google API console project:
   a. Access the Admin console by clicking Google Admin in the top menu.
   b. In the Admin console, click Security.
   c. In the Security page, click Show more, and then select Advanced Settings > Manage API client access.
   d. In the Manage API client access page:
      i. In the Client Name box, enter the previously obtained Client ID from the Google Console (see Authorizing the Coveo Connector to Access Your Users Gmail Mailboxes).
      ii. In the One or More API Scopes box, enter:
**Note:** When you use the same Google Developer Console project as another Coveo connector (Google Drive for Work or Google Drive for Work Compact), you must reenter its API scopes here (https://docs.google.com/feeds/, https://www.googleapis.com/auth/drive.readonly, https://www.googleapis.com/auth/userinfo.email and https://www.googleapis.com/auth/admin.directory.group.readonly).

If not, adding the following two Gmail scopes will remove the ones that were already added for this Client ID.

- https://www.googleapis.com/auth/gmail.readonly
- https://www.googleapis.com/auth/admin.directory.user.readonly

iii. Click **Authorize**.

### 9.16.6 Configuring and Indexing a Gmail for Work Source

A source defines a set of configuration parameters for a specific Google Apps for Work account.

To configure and index a Gmail for Work source

1. On the Coveo server, access the Administration Tool.

2. Select **Index > Sources and Collections**.

3. In the **Collections** section:
   a. Select an existing collection in which you want to add the new source.

   OR

   b. Click **Add** to create a new collection.

4. In the **Sources** section, click **Add**.

   The **Add Source** page that appears is organized in three sections.

5. In the **General Settings** section of the **Add Source** page:
a. Enter the appropriate value for the following required parameters:

**Name**

Enter a descriptive name of your choice for the connector source.

*Example: Gmail for Work*

**Source Type**

Select the connector used by this source. In this case, select **Gmail (Google Apps)**.

*Note: If you do not see Gmail (Google Apps), your environment does not meet the requirements (see "Gmail for Work Connector Requirements" on page 966).*

**Addresses**

This parameter is not used, but must not be empty. Enter `http://www.gmail.com`.

**Fields**

Select the field set that you created for your Gmail source (see Gmail for Work Connector Deployment Overview).

**Refresh Schedule**

Time interval at which the index is automatically refreshed to keep the index content up-to-date. By default, the **Every day** option instructs CES to refresh the source everyday at 12 AM. Because the incremental refresh takes care of maintaining the source up-to-date, you can select a longer interval such as **Every Sunday**.
b. Review the value for the following parameters that often do not need to be modified:

**Rating**

Change this value only when you want to globally change the rating associated with all items in this source relative to the rating to other sources.

*Example:* When a source replaces a legacy system, you may want to set this parameter to **High**, so that in the search interface, results from this source appear earlier in the list compared to those from legacy system sources.

**Document Types**

If you defined a custom document type set for this source, select it.

**Active Languages**

If you defined custom active language sets, ensure to select the most appropriate for this source.

6. In the **Specific Connector Parameters & Options** section of the **Add Source** page:

   ![Specific Connector Parameters & Options](image)

   a. Using the following parameters, authorize the Coveo crawler to access the Gmail mailbox of your users:

   **Domain(s)**

   Enter the Gmail domain that you want to index. When your Google Apps account contains more than one domain, you can enter a semicolon-separated list of domains to index.

   *Examples:*

   - One domain: mydomain.com
   - Multiple domains: myfirstdomain.com;my.second.domain.com

   **Service account e-mail**

   Enter the service account **Email address** previously obtained (see **Authorizing the Coveo Connector to**
Access Your Users Gmail Mailboxes).

**Example:** 12345678901@developer.gserviceaccount.com

**User admin account e-mail**

Enter the domain admin account (Read check box is selected for Users under Admin API Privileges) email used to obtain the list of users in the domain.

**Example:** admin@domain.com

**Service account PCKS12 file path**

Enter the path on the Coveo Master server where you saved the previously obtained service account's PCKS12 private key file (see Authorizing the Coveo Connector to Access Your Users Gmail Mailboxes).

**Example:** D:\CES7\Config\1234ab8e315e67a89e02f16ea38bd44d609471ff-privatekey.p12

b. In the Mapping File box, leave the default value to use the default mapping file that comes with the connector (Coveo.CES.CustomCrawlers.Gmail.MappingFile.xml). If you create a custom mapping file, enter the full path to your custom mapping file. Contact Coveo Support for assistance if you need to customize the mapping file.

c. Click Add Parameter when you want to show and change the value of advanced source parameters (see "Modifying Hidden Gmail for Work Source Parameters" on page 978).

**Example:** In the case you do not want spam messages to be indexed, you must add the IncludeSpamTrashMessage hidden parameter (see IncludeSpamTrashMessage).

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Name</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>IncludeSpamTrashMessage</td>
<td>false</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th></th>
<th>Add Parameter</th>
</tr>
</thead>
</table>

- **d.** The Option check boxes generally do not need to be changed:

  **Index Subfolders**

  This parameter is not taken into account for this connector.

  **Index the document's metadata**

  When selected, CES indexes all the document metadata, even metadata that are not associated with a field. The orphan metadata are added to the body of the document so that they can be searched using free text queries.

  When cleared (default), only the values of system and custom fields that have the Free Text Queries attribute selected will be searchable without using a field query.
Example: A document has two metadata:
- `LastEditedBy` containing the value Hector Smith
- `Department` containing the value RH

In CES, the custom field `CorpDepartment` is bound to the metadata `Department` and its **Free Text Queries** attribute is selected.

When the **Index the document's metadata** option is cleared, searching for RH returns the document because a field is indexing this value. Searching for hector does not return the document because no field is indexing this value.

When the **Index the document's metadata** option is selected, searching for hector also returns the document because CES indexed orphan metadata.

**Document's addresses are case-sensitive**

Leave the check box cleared. This parameter needs to be checked only in rare cases for case sensitive systems in which distinct documents may have the same file name but with different casing.

**Generate a cached HTML version of indexed documents**

When you select this check box (recommended), at indexing time, CES creates HTML versions of indexed documents. In the search interfaces, users can then more rapidly review the content by clicking the **Quick View** link rather than opening the original document with the original application. Consider clearing this check box only when you do not want to use **Quick View** links or to save resources when building the source.

**Open results with cached version**

Leave this check box cleared (recommended) so that in the search interfaces, the main search result link opens the original document with the original application. Consider selecting this check box only when you do not want users to be able to open the original document but only see the HTML version of the document as a **Quick View**. In this case, you must also select **Generate a cached HTML version of indexed documents**.

7. In the **Security** section of the **Add Source** page:

   ![Security](image)

   a. In the **Security Provider** drop-down list, select the security provider that you created for this source (see [Gmail for Work Connector Deployment Overview](https://www.coveo.com)).

8. Click **Save** to save the source configuration.

9. When you are ready to start indexing the Gmail source, click **Rebuild**.
10. Validate that the source building process is executed without errors:
   - In the navigation panel on the left, click Status, and then validate that the indexing proceeds without errors.
   - OR
   - Open the CES Console to monitor the source building activities.

What's Next?

Set an incremental refresh schedule for your source.

Consider modifying some hidden source parameters to try resolving other issues (see "Modifying Hidden Gmail for Work Source Parameters" on page 978).

9.16.6.1 Modifying Hidden Gmail for Work Source Parameters

The Add Source and Source: ... General pages of the Administration Tool present the parameters with which you can configure the connector for most Gmail for Work setups. More advanced and more rarely used parameters are hidden. You can choose to make one or more of these parameters appear in the Add Source and Source: ... General pages of the Administration Tool so that you can change their default value. Consider changing values of hidden parameters when you encounter issues.

The following list describes the advanced hidden parameters available with Gmail for Work sources. The parameter type (integer, string, etc.) appears between parentheses following the parameter name.

**HttpTimeoutInMs (Integer)**

The timeout value (in milliseconds) allowed for a HTTP request to complete. The default value is 100000 milliseconds.

**NumberOfRefreshThreads (Integer)**

The number of refresh threads used by the crawler for this source. The default value is 1.

**NumberOfRetries (Integer)**

The number of retries allowed when a recoverable call to Google API fails. The default value is 3.

**UsersToCrawl (String)**

The email address of the user (or a semicolon separated list of users email) you want to index the Gmail mailbox content. By default, the mailbox of every user under the Google Apps for Work domain is indexed.

**IncludeSpamTrashMessage (Boolean)**

Whether to include messages from the Spam and Trash folders in the results. The default value is true.

To modify hidden Gmail for Work source parameters

1. Refer to "Adding an Explicit Connector Parameter" on page 450 to add one or more Gmail for Work source parameters.

2. For a new Gmail for Work source, access the Add Source page of the Administration Tool to modify the value
of the newly added advanced parameter:
   a. Select Index > Sources and Collections.
   b. Under Collections, select the collection in which you want to add the source.
   c. Under Sources, click Add.
   d. In the Add Source page, edit the newly added advanced parameter value.

3. For an existing Gmail for Work source, access the Source: ... General page of the Administration Tool to modify the value of the newly added advanced parameter:
   a. Select Index > Sources and Collections.
   b. Under Collections, select the collection containing the source you want to modify.
   c. Under Sources, click the existing Gmail for Work source in which you want to modify the newly added advanced parameter.
   d. In the Source: ... General page, edit the newly added advanced parameter value.

4. Rebuild your Gmail for Work source to apply the changes to the parameters.

9.17 Google Drive for Work Compact Connector

CES 7.0.7599+ (April 2015)

The Coveo connector for Google Drive for Work allows Coveo administrators to index and integrate Google Drive for Work content into the Coveo unified index. The connector indexes all items and the attached permissions from all Google Drive domain users so that in the Coveo search interfaces, a user can easily find any but only content to which he has access in Google Drive.

9.17.1 Connector Features Summary

<table>
<thead>
<tr>
<th>Features</th>
<th>Supported</th>
<th>Additional information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Google Drive for Work version</td>
<td>Latest cloud version</td>
<td>Following available Google Drive for Work releases</td>
</tr>
<tr>
<td>Searchable content types¹</td>
<td>✔️</td>
<td>Files, folders, comments and replies², and user profiles</td>
</tr>
<tr>
<td>Content update</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Incremental refresh</td>
<td>✔️</td>
<td></td>
</tr>
<tr>
<td>Full refresh</td>
<td>✔️</td>
<td></td>
</tr>
<tr>
<td>Rebuild</td>
<td>✔️</td>
<td></td>
</tr>
<tr>
<td>Document-level security</td>
<td>✔️</td>
<td></td>
</tr>
</tbody>
</table>
1- **By default the Drive for Work source includes files of the My Drive folder for each user.** Shared documents are included with the associated permissions, so that who ever is authorized to see the items can find them in Coveo search results.

2- The comments and replies are included in the `coveo.comments` and `coveo.comments.authors` metadata of their parent item rather than as separate items. This way, users can search for the content of a comment or reply and find the parent document.

### 9.17.2 Features

The Google Drive for Work Compact connector features are:

**Content indexing**

Extraction and indexing of all Google Drive object types:
- User profile
- Folders
- Files
- Comments and replies

**Note:** The comments and replies are indexed in the `coveo.comments` and `coveo.comments.authors` metadata of their parent document rather than as separate documents. This way, users can search for the content of a comment or reply and find the parent document.

**Note:** By default the Google Drive for Work Compact connector indexes files of the My Drive folder for each user. Shared documents are included with the associated permissions, so that who ever is authorized to see the documents can find them in Coveo search results.

**Fully supported security model**

The connector fully supports the Google Drive security model using a security provider to get permissions for each indexed item. This means that, in Coveo search interfaces, a user searching Google Drive content only sees the content to which he has access.

**Incremental refresh**

Supports incremental refresh to periodically query Google Drive for the latest edits, keeping the index content up-to-date.

**Out-of-the-box configuration**

The connector is ready to use with minimal configuration to indicate which items to index and which metadata to use.

**Multithreading**

The connector can run multiple threads, which can improve performances considerably (see Modifying Hidden Google Drive for Work Compact Source Parameters).
What's Next?

Review the steps to deploy the Google Drive for Work Compact connector (see "Google Drive for Work Compact Connector Deployment Overview" on page 981).

9.17.3 Google Drive for Work Compact Connector Deployment Overview

The following procedure outlines the steps needed to deploy the Google Drive for Work Compact connector. The steps indicate the order in which you must perform configuration tasks on both the Google and Coveo servers.

To deploy the Google Drive for Work Compact connector:

1. Validate that your environment meets the requirements (see "Google Drive for Work Compact Connector Requirements" on page 982).

2. On the Google server:
   a. Create a Google API Console project to authorize the Coveo connector to access the Google Drive of your users (see "Authorizing the Coveo Connector to Access Your Google Drive" on page 983).
   b. Modify security parameters in your Google Apps account to grant the connector access to your Google Apps for Work (see "Authorizing the Coveo Connector to Access Your Google Apps for Work" on page 987).

3. On the Coveo server, in the Coveo Administration Tool:
   a. Optionally create security providers

      When you want to index Google Drive permissions, you must create two security providers to get Google Apps for Work item permissions and resolve and expand groups.

      In Google Drive, users are identified by their email addresses. Consequently, permissions returned by the Google Apps for Work security provider for each document are email addresses. The Google Apps for Work security provider then requires another security provider to uniquely identify users from their email addresses.

      i. Start by selecting or creating an Email or an Active Directory security provider that the Google Apps for Work security provider will use to resolve and expand groups. The security provider type to use depends on how users are authenticated when they access the search interface:

         - When authenticated with their email address, use an Email security provider (see "Configuring an Email Security Provider" on page 65).
         - When authenticated with an Active Directory account, use an Active Directory security provider (see "Configuring an Active Directory Security Provider" on page 1141).
Notes:

- CES comes with an Active Directory security provider that you can configure to connect to the default domain. When your environment contains more than one domain, you can select an Active Directory security provider that you created for other domains.

- An Active Directory security provider is appropriate only when the User Principal Name (UPN) matches the email address for all users.

Note: You may require to also use a REGEX Transform Member Name security provider in between the two other security providers to map member types. Contact Coveo Support for assistance.

ii. Then create a Google Apps for Work security provider that the connector uses to resolve indexed permissions (see "Configuring a Google Drive for Work Compact Security Provider" on page 988).

b. Create a Google Drive field set to take advantage of the available Google Drive metadata.

i. It is recommended to start by importing the default Google Drive field set file ([CES_Path]Bin\Coveo.CES.CustomCrawlers.GoogleDrive.FieldSet.xml) to create fields for all the metadata available by default from Google Drive documents.

Note: CES 7.0.7711+ (June 2015) A second version of the field set containing the coveo.folding.child and systo fields is available.

ii. When you created custom metadata for your Google Drive documents, add corresponding fields to the field set.

c. Configure and index a Google Drive for Work source.

The connector must know details about the authorized access to the Google Drive of your users to index its content (see "Configuring and Indexing a Google Drive for Work Compact Source" on page 991).

d. If you encounter issues, verify if modifying the default value of hidden source parameters can help resolve the problems (see "Modifying Hidden Google Drive for Work Compact Source Parameters" on page 996).

9.17.4 Google Drive for Work Compact Connector Requirements

Your environment must meet the following requirements to be able to use the Google Drive for Work Compact connector:

- CES 7.0.7599+ (April 2015)

- Coveo license for the Google Drive Compact (Google Apps for Work) connector

  Your Coveo license must include support for the Google Drive for Work Compact connector to be able to use this connector.

- A valid Google Account

  Using a Google Account with administrator privilege, you must log in the Google API Console to authorize Coveo to access the Google Drive of your users (see Authorizing the Coveo Connector to Access Your Google Drive).
Administrator credentials to your Google Apps account

You must log in to your Google Apps account to modify security options and authorize Coveo to access your Google Apps for Work (see Authorizing the Coveo Connector to Access Your Google Apps for Work).

Google Drive storage licenses for your Google Apps users

In your Google Apps account, you must activate the Google Drive service (see Authorizing the Coveo Connector to Access Your Google Apps for Work).

Coveo Master server free disk space for temporary files

Before indexing your Google Drive, ensure that your Coveo Master server has sufficient free hard disk space to temporarily store indexed Google Drive content.

The Google Drive connector creates a BLOB store on the Coveo Master server ([CES_Path]\Index\Crawlers\BlobStore or [CES_Path]\Index\Crawlers\BlobStore32) where shared downloaded documents with sizes greater than 100 KB are temporarily saved. This mechanism prevents downloading and re-indexing all copies of shared documents and allows to index metadata associated with each shared document copy.

What's Next?

Grant Coveo access to the Google Drive of your users by creating a Google API Console project and modifying security options in your Google Apps account (see "Authorizing the Coveo Connector to Access Your Google Drive" on page 983).

9.17.5 Setting Google Permissions (Google Drive for Work)

Before you start configuring the Google Drive for Work Compact Coveo connector, you must first set appropriate Google permissions.

Refer to the following topics to perform the necessary Google security configuration:

1. "Authorizing the Coveo Connector to Access Your Google Drive" on page 983
2. "Authorizing the Coveo Connector to Access Your Google Apps for Work" on page 987

9.17.5.1 Authorizing the Coveo Connector to Access Your Google Drive

You must perform a G Suite domain-wide delegation of authority to authorize the Coveo connector to access the Google Drive content that you want to index.

To authorize the connector to access the Google Drive of your users

1. Go to the Google Developers Console, and log in using a Google Account with administrator credentials.
2. At the left of the **Filter by name, ID or label** input, click the drop-down menu, and then select the organization in which you want to create the Google Developer Console project.

3. Create an API project for the Coveo connector (CES 7) or source (Coveo Cloud):
   a. In the **Manage resources** panel, click **Create a project**.
   b. (When your project limit is exceeded) In the **Increase Project Limit** page, click **Request increase**, and then complete the form.
   c. In the **New Project** dialog page, enter the project required information:

   ![New Project dialog](image)

   i. Enter a **Project name**.

   **Note**: The project ID is automatically created based on the project name. You can always modify the project ID by clicking **Edit**.

   ii. (When you create the first project in your organization only) Answer the **Please email me updates regarding feature announcements, performance suggestions, feedback surveys and special offers** question using the **Yes** or **No** checkbox.

   iii. (When you create the first project in your organization only) After you have read and agree to the **Google Play Android Developer API Terms of Service**, click the **Yes** check box.

   iv. Click **Create**.

4. Enable the required Google APIs:
   a. Access the API **Library** page by clicking **Google APIs** in the top menu.
   b. In the API **Library** page, enable the **Gmail API** and **Admin SDK** APIs:
Under **Google APIs**, use the search box to search and select **Google Drive API** or **Admin SDK**.

ii. In the **Google Drive API** or **Admin SDK** page, in the action bar, click **Enable**.

iii. In the action bar, click the back button (←).

iv. Repeat the procedure for the other API.

5. Create a service account project for the Coveo connector (CES 7) or source (Coveo Cloud).

   a. In the sidebar on the left, select **Credentials**.

   b. In the **Credentials** page, click the **Create credentials** drop-down list menu, and then select **Service account key**.

   c. In the **Create service account key** page:

      i. Click the **Service account** drop-down list menu, and then select **New service account**.

      ii. Click the **Role** drop-down list menu, and then select **Service account > Service account admin**.

      iii. In the first box, enter a **Service account name**.

         **Example:** Coveo Connector

      iv. (Optionally) Edit the **Service account ID** or generate another one by clicking the refresh icon ✿.

         **Note:** The service account ID is automatically created based on the service account name.

      v. Under **Key type**, select **P12**.

      vi. Click **Create**.
vi. In the **New private key** dialog box that appears, take note of the private key password, and then click **Close**.

6. (For CES 7 customers only) Using an administrator account, connect to your Coveo Master server, and then copy the downloaded private key [GUID]-privatekey.p12 file to a folder accessible to Coveo Enterprise Search, typically in the [Index_Path]\Config folder.

7. Back in the **Credentials** page, perform a G Suite domain-wide delegation.
   a. At the top right of the **Service account keys** table, click **Manage service accounts**.
   b. At the right end of your service account row, click the more icon (・), and then select **Edit**.
   c. In the **Edit service account** dialog that appears:
      i. Click the **Enable G Suite Domain-wide Delegation** check box
      ii. In the **Product name for the consent screen** box, enter the product name (e.g., Coveo Connector) that will appear when the application requests read access to the users’ data.
      iii. Click **Save**.

8. Back in the **Service Accounts** page, on the service account row you just created, in the **Options** column of your service account row, click **View Client ID**.

9. In the **Client ID Service account client** page, then take note of the following information that you will need later to configure your Google Drive for Work source:
   - **Client ID**
   - **Email address** (under the **Service account** name)
What's Next?

You must modify security parameters in your Google Apps account to grant the connector access to your Google Apps for Work (see "Authorizing the Coveo Connector to Access Your Google Apps for Work" on page 987).

9.17.5.2 Authorizing the Coveo Connector to Access Your Google Apps for Work

You must perform a Google Suite domain-wide delegation of authority to authorize the Coveo connector (CES 7) or source (Coveo Cloud) to access your Google Apps for Work.

To authorize the connector to access your Google Apps for Work

1. Go to your Google Apps for Work domain Admin console:
   a. Access the User hub with an administrator account.
   b. In the hub, click Admin Console.

2. In the Google Admin Console, click Apps.

3. In the Apps page, select Google Suite.

4. In the Google Apps page, ensure that for Drive and Docs, the Status is set to On for everyone.

5. Grant access to users data for the Google API console project:
   a. Access the Admin console by clicking Google Admin in the top menu.
   b. In the Admin console, click Security.
c. In the Security page, click Show more, and then select Advanced Settings > Manage API client access.

d. In the Manage API client access page:
   i. In the Client Name box, enter the previously obtained Client ID from the Google Console (see Authorizing the Coveo Connector to Access Your Google Drive).
   ii. In the One or More API Scopes box, enter the following list of values, separating each with a comma:

   **Note:** When you use the same Google Developer Console project as another Coveo connector (i.e., Gmail for Work), you must reenter its scope here (https://www.googleapis.com/auth/gmail.readonly). If not, adding the following scopes will remove the ones that were already added for this Client ID.

   - https://docs.google.com/feeds/
   - https://www.googleapis.com/auth/drive.readonly
   - https://www.googleapis.com/auth/userinfo.email
   - https://www.googleapis.com/auth/admin.directory.user.readonly
   - https://www.googleapis.com/auth/admin.directory.group.readonly

   iii. Click Authorize.

9.17.6 Configuring a Google Drive for Work Compact Security Provider

The Coveo Google Drive for Work Compact connector fully supports the Google security model. When you want users searching for Google Drive content in a Coveo search interface to only see the content to which they have access in Google Drive, the connector needs a security provider to be able to index the permissions for each indexed Google Drive item.

**Note:** You can get familiar with how Coveo components deal with permissions on documents both at indexing and query time.

To configure a Google Drive for Work Compact security provider

1. On the Coveo server, access the Administration Tool.
3. In the navigation panel on the left, click **Security Providers**.

4. In the **Security Providers** page, click **Add** to create a new security provider.

5. In the **Modify Security Provider** page:

   ![Modify Security Provider](image)

   a. Configure the following required parameters:

   **Name**
   
   Choose a meaningful name to identify the security provider.

   **Example**: Google Drive for Work Compact Security Provider

   **Security Provider Type**
   
   In the drop-down list, select **Google Apps (x64)**.

   **User Identity**
   
   In the drop-down list, select **(none)**.
Activate domain-wide mode

You must select this option when you plan to use this security provider with a Google Drive Compact (Google Apps) source type.

Security Provider

Select the security provider that you selected or created to allow this security provider to resolve and expand the groups (see Google Drive for Work Compact Connector Deployment Overview).

b. Configure the following required parameters with the same values as the ones you will enter when configuring the source (see “Configuring and Indexing a Google Drive for Work Compact Source” on page 991):

[Domain-wide mode] Managed domains

Enter the domain that you want to index. When your Google Apps account contains more than one domain, you can enter a semicolon-separated list of domains to index. The security provider will resolve and expand groups for the specified domain(s).

Examples:
- One domain: mysubdomain.mycompany.com
- Multiple domains: myfirstdomain.com;myseconddomain.com

Service Account Email

Enter the service account Email address previously obtained (see Authorizing the Coveo Connector to Access Your Google Drive).

Example: 12345678901@developer.gserviceaccount.com

Certificate File Path

Note: This parameter can be left empty when you use the CertificateFileData hidden parameter (see CertificateFileData).

Enter the path on the Coveo Master server where you saved the previously obtained service account's PCKS12 private key file (see Authorizing the Coveo Connector to Access Your Google Drive).

Example: D:\CES7\Config\1234ab8e315e67a89e02f16ea38bd44d609471ff-privatekey.p12

Domain Administrator Email

Enter the domain admin account email used to obtain the list of users in the domain.

Example: admin@domain.com

c. Leave the Allow Complex Identities cleared as it does not apply to this type of security provider.

d. Click Apply Changes.
What's Next?

Create and index a source (see "Configuring and Indexing a Google Drive for Work Compact Source" on page 991).

9.17.7 Configuring and Indexing a Google Drive for Work Compact Source

A source defines a set of configuration parameters for a specific Google Apps for Work account.

To configure and index a Google Drive for Work source

1. On the Coveo server, access the Administration Tool.
2. Select **Index > Sources and Collections**.
3. In the **Collections** section:
   a. Select an existing collection in which you want to add the new source.
   
   OR

   b. Click **Add** to create a new collection.
4. In the **Sources** section, click **Add**.

   The **Add Source** page that appears is organized in three sections.
5. In the **General Settings** section of the **Add Source** page:
a. Enter the appropriate value for the following required parameters:

**Name**

Enter a descriptive name of your choice for the connector source.

*Example:* Google Drive for Work Compact

**Source Type**

Select the connector used by this source. In this case, select Google Drive Compact (Google Apps).

*Note:* If you do not see Google Drive Compact (Google Apps), your environment does not meet the requirements (see "Google Drive for Work Compact Connector Requirements" on page 982).

**Addresses**

This parameter is not used, but must not be empty. Enter http://www.google.com.

**Fields**

Select the field set that you created for your Google Drive Compact source (see Google Drive for Work Compact Connector Deployment Overview).

**Refresh Schedule**

Time interval at which the index is automatically refreshed to keep the index content up-to-date. By default, the *Every day* option instructs CES to refresh the source everyday at 12 AM. Because the incremental refresh takes care of maintaining the source up-to-date, you can select a longer interval such as *Every Sunday*.

b. Review the value for the following parameters that often do not need to be modified:

**Rating**

Change this value only when you want to globally change the rating associated with all items in this source relative to the rating to other sources.

*Example:* When a source replaces a legacy system, you may want to set this parameter to *High*, so that in the search interface, results from this source appear earlier in the list compared to those from legacy system sources.

**Document Types**

If you defined a custom document type set for this source, select it.

**Active Languages**

If you defined custom active language sets, ensure to select the most appropriate for this source.

6. In the **Specific Connector Parameters & Options** section of the **Add Source** page:
a. In the **Mapping File** box, optionally enter the path to a mapping file that should apply to the items in this source.

Leave this box empty to use the default mapping that should be appropriate in most cases.

When the default mapping does not fulfill your needs, contact Coveo Support for assistance. Your XML mapping file must respect the standard Coveo mapping file schema.

**Example:** D:\CES7\Config\GoogleAppsMappingFile.xml

b. Using the following parameters, authorize the Coveo crawler to access the Google Drive of your users:

**Domain Admin e-mail**

Enter the domain admin account email used to obtain the list of users in the domain.

**Example:** admin@domain.com

**Note:** The e-mail you enter here must be the same as the one you entered previously when configuring the security provider (see Configuring a Google Drive for Work Compact Security Provider).

**Domain(s)**

Enter the Google Drive domain that you want to index. When your Google Apps account contains more than one domain, you can enter a semicolon-separated list of domains to index.

**Examples:**

- **One domain:** mydomain.com
- **Multiple domains:** myfirstdomain.com;my.second.domain.com
Important: The domain(s) specified in this list must match the one(s) specified in the security provider [Domain-wide mode] Managed domains list (see Configuring a Google Drive for Work Compact Security Provider).

Service account e-mail

Enter the service account Email address previously obtained (see Authorizing the Coveo Connector to Access Your Google Drive). It must be the same email that you entered when configuring the security provider (see Configuring a Google Drive for Work Compact Security Provider).

Example: 12345678901@developer.gserviceaccount.com

Service account PCKS12 file path

Note: This parameter is no longer required and can be left empty when you use the ServiceAccountPcks12FileData hidden parameter (see Modifying Hidden Google Drive for Work Compact Source Parameters).

Enter the path on the Coveo Master server where you saved the previously obtained service account's PCKS12 private key file (see Authorizing the Coveo Connector to Access Your Google Drive). It must be the same path that you entered when configuring the security provider (see Configuring a Google Drive for Work Compact Security Provider).

Example: D:\CES7\Config\1234ab8e315e67a89e02f16ea38bd44d60947ff-privatekey.p12

c. Select the type of content to index using the following options:

Crawl trashed items

Select to index the items in the user's trash. Not selected by default.

Crawl custom properties

Select to index custom properties that Google applications or your custom applications added on items. Not selected by default.

Note: Crawling custom properties adds one API call per indexed document. Selecting this option can notably increase the number of calls to the Google Drive API and the crawling time.

Index Users [CES 7.0.9167+ (December 2017)]

Select to index Google Drive users as separate documents. Not selected by default.

d. Click Add Parameter when you want to show and change the value of advanced source parameters (see "Modifying Hidden Google Drive for Work Compact Source Parameters" on page 996).

e. The Option check boxes generally do not need to be changed:

Index Subfolders

This parameter is not taken into account for this connector.
Index the document’s metadata

When selected, CES indexes all the document metadata, even metadata that are not associated with a field. The orphan metadata are added to the body of the document so that they can be searched using free text queries.

When cleared (default), only the values of system and custom fields that have the Free Text Queries attribute selected will be searchable without using a field query.

**Example:** A document has two metadata:

- LastEditedBy containing the value Hector Smith
- Department containing the value RH

In CES, the custom field CorpDepartment is bound to the metadata Department and its Free Text Queries attribute is selected.

When the Index the document's metadata option is cleared, searching for RH returns the document because a field is indexing this value. Searching for hector does not return the document because no field is indexing this value.

When the Index the document's metadata option is selected, searching for hector also returns the document because CES indexed orphan metadata.

Document’s addresses are case-sensitive

Ensure that this option is selected because Google Drive document IDs are case sensitive.

Generate a cached HTML version of indexed documents

When you select this check box (recommended), at indexing time, CES creates HTML versions of indexed documents. In the search interfaces, users can then more rapidly review the content by clicking the Quick View link rather than opening the original document with the original application. Consider clearing this check box only when you do not want to use Quick View links or to save resources when building the source.

Open results with cached version

Leave this check box cleared (recommended) so that in the search interfaces, the main search result link opens the original document with the original application. Consider selecting this check box only when you do not want users to be able to open the original document but only see the HTML version of the document as a Quick View. In this case, you must also select Generate a cached HTML version of indexed documents.

7. In the Security section of the Add Source page:
a. When you chose to index Google Drive permissions, in the **Security Provider** drop-down list, select the Google Drive for Work Compact security provider that you created for this source (see "Configuring a Google Drive for Work Compact Security Provider" on page 988).

b. In the **Authentication** drop-down list, select (none).

8. Click **Save** to save the source configuration.

9. When you chose to not index Google Drive permissions, you can set source level permissions that apply to all documents in the source:

   a. In the navigation panel on the left, click **Permissions**.

   b. In the **Permissions** page, select **Specify the security permissions** to index.

   c. In the **Allowed Users** and **Denied Users** boxes, enter the users and groups that you respectively want to allow or deny to see search results from this source. The default is to allow everyone \S-1-1-0\ (Active Directory Group).

   d. Click **Apply Changes**.

10. When you are ready to start indexing the Google Drive source, click **Rebuild**.

11. Validate that the source building process is executed without errors:

   - In the navigation panel on the left, click **Status**, and then validate that the indexing proceeds without errors.

   OR

   - Open the CES Console to monitor the source building activities.

**What's Next?**

Set an incremental refresh schedule for your source.

Consider modifying some hidden source parameters to try resolving other issues (see "Modifying Hidden Google Drive for Work Compact Source Parameters" on page 996).

**9.17.8 Modifying Hidden Google Drive for Work Compact Source Parameters**

The **Add Source** and **Source: ... General** pages of the Administration Tool present the parameters with which you can configure the connector for most Google Drive for Work setups. More advanced and more rarely used parameters are hidden. You can choose to make one or more of these parameters appear in the **Add Source** and
Source: ... General pages of the Administration Tool so that you can change their default value. Consider changing values of hidden parameters when you encounter issues.

The following list describes the advanced hidden parameters available with Google Drive for Work Compact sources. The parameter type (integer, string, etc.) appears between parentheses following the parameter name.

**IgnoreLinkRequiredPermissions (Boolean)** CES 7.0.8225.5+ (Mars 2016)

Whether to ignore permissions with a required link on the documents. The default value is true.

Notes:
- Permissions requiring links are either "Anyone with the link" or "Anyone at <domain> with the link" (see Share Google Drive files and folders).
- By default, in a Coveo search page, end-users cannot find Google Drive documents in search results with either the "Anyone with the link" or "Anyone at <domain> with the link" permissions.

**NumberOfRefreshThreads (Integer)**

The number of refresh threads used by the crawler for this source. The default value is 8.

**ResultsPerPage (Integer)**

Number of results to fetch per request made to Google Drive. The default value is 100. The minimum value is 1 and the maximum value is 1000. A small value (not recommended) forces the connector to make small but frequent queries to Google Drive. A larger value (recommended) leads to larger and less frequent queries.

Note: Queries to the Google Drive service are made per folder.

Example: With a value of 100, if a folder contains 180 items, two queries will be necessary to obtain the items.

**CommentsPerPage (Integer)**

Number of comments to fetch per request made to Google Drive. The default and maximum value is 100. The minimum value is 1.

**CrawlSharedWithMeItems (Boolean)**

Whether to process items that have been shared with each user (Shared with me). The default value is true.

**CrawlComments (Boolean)**

Whether to index comments from each item. The default value is false. Consider setting this parameter to true when you must have searchable comments. However, make comments searchable costs API calls and can increase crawling time depending on the number of comments in your Google Drive content.

**UseFolderLinksInMyDrive (Boolean)**

Whether to use folder links that open directly in My Drive rather than in a folder view. The default value is true.
Example: In the search results breadcrumb for a Shared with me document, when a user clicks the parent folder and this parameter is set to false, the opened URL is in the form https://drive.google.com/a/mydomain.com/folderview?id=[GUID]&usp=drivesdk#, showing a file and folder view with a Open in My Drive link.

When set to true, the opened URL is in the form https://drive.google.com/a/mydomain.com/?usp=folder#folders/[GUID], directly opening in My Drive, as if the user had clicked the Open in My Drive link, thus saving one click.

IndexGoogleAppsDocThumbnails (Boolean)

Whether to index thumbnails for Google Apps for Work documents. The default value is false. Setting this parameter to true to index document thumbnails would increase the crawling time by about 5%.

IndexNativeDocThumbnails (Boolean)

Whether to index thumbnails for native documents (PDF, DOC, XLS, etc.). The default value is false.

AddFromAndToFields (Boolean)

Whether to add the sysfrom and systo fields to system fields. The default value is true. Adding these fields can have a significant impact on the crawling performance, so consider setting this parameter to false to improve crawling performance.

EnablePrefetcher (Boolean)

Whether the prefetcher is used by the crawler. The default value is false in which case the connector processes the items of a folder retrieved with an API call before making the next API call for the next Google Drive folder.

It is recommended to enable the prefetcher that immediately makes the next API call and improves crawling performances, particularly when folders contain many documents.

NumberOfPrefechedItems (Integer)

The maximum number of items to prefetch will save in memory when the prefetcher is enabled (see "EnablePrefetcher (Boolean)" on page 998). The default value is 300. The minimum value is 1 and the maximum value is 1000.

Consider increasing the NumberOfPrefechedItems value if you increase the number of threads used by the crawler (see NumberOfRefreshThreads).

ServiceAccountPkcs12FileData (Integer)

The service account's PKCS12 private key file encoded data. The PKCS12 file encoded in Base64. The default value is null.
Notes:

- You need to open the certificate in a text editor and use an encoding application such as Motobit to convert the certificate content to the Base64 format.
- This parameter is only used when the Service account PKCS12 file path parameter is empty (see Configuring and Indexing a Google Drive for Work Compact Source).

**FileMimeTypesWithComments** *(String)* **CES 7.0.7914+ (October 2015)*

Semicolon separated list of document MIME types which support comments in Google Drive (see Supported MIME Types). The default value is application/vnd.google-apps.document;application/vnd.google-apps.presentation;application/vnd.google-apps.spreadsheet;application/vnd.google-apps.drawing.

To modify hidden Google Drive for Work Compact source parameters

1. Refer to "Adding an Explicit Connector Parameter" on page 450 to add one or more Google Drive for Work Compact source parameters.

2. For a new Google Drive for Work Compact source, access the Add Source page of the Administration Tool to modify the value of the newly added advanced parameter:
   a. Select Index > Sources and Collections.
   b. Under Collections, select the collection in which you want to add the source.
   c. Under Sources, click Add.
   d. In the Add Source page, edit the newly added advanced parameter value.

3. For an existing Google Drive for Work Compact source, access the Source: ... General page of the Administration Tool to modify the value of the newly added advanced parameter:
   a. Select Index > Sources and Collections.
   b. Under Collections, select the collection containing the source you want to modify.
   c. Under Sources, click the existing Google Drive for Work Compact source in which you want to modify the newly added advanced parameter.
   d. In the Source: ... General page, edit the newly added advanced parameter value.

4. Rebuild your Google Drive for Work Compact source to apply the changes to the parameters.

**9.18 Google Drive for Work Connector**

**CES 7.0.5989+ (October 2013)*

The Coveo beta connector for Google Drive for Work allows Coveo administrators to index and integrate the Google Drive content into the Coveo unified index. The connector indexes all items and the attached permissions from all Google Drive domain users so that in the Coveo search interfaces, a user can easily find any but only content to which he has access in Google Drive.
9.18.1 Connector Features Summary

<table>
<thead>
<tr>
<th>Features</th>
<th>Supported</th>
<th>Additional information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Google Drive for Work version</td>
<td>Latest cloud version</td>
<td>Following available Google Drive for Work releases</td>
</tr>
<tr>
<td>Searchable content types¹</td>
<td>✓</td>
<td>Files, folders, comments and replies², and user profiles</td>
</tr>
<tr>
<td>Content update</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Incremental refresh</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Full refresh</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Rebuild</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Document-level security</td>
<td>✓</td>
<td></td>
</tr>
</tbody>
</table>

1- **By default** the Drive for Work source includes files of the **My Drive** folder for each user. **Shared documents are included with the associated permissions, so that whoever is authorized to see the items can find them in Coveo search results.**

2- **The comments and replies are included in the coveo.comments and coveo.comments.authors metadata of their parent item rather than as separate items. This way, users can search for the content of a comment or reply and find the parent document.**

9.18.2 Features

The Google Drive for Work connector features are:

**Content indexing**

- Extraction and indexing of all Google Drive object types:
  - User profile
  - Folders
  - Files
  - Comments and replies

**Note:** CES 7.0.6830+ (July 2014) The comments and replies are indexed in the coveo.comments and coveo.comments.authors metadata of their parent document rather than as separate documents. This way, users can search for the content of a comment or reply and find the parent document.
**Note:** By default the Google Drive for Work connector indexes the content of the My Drive and Shared with me folders for each user. To minimize reindexing several times the same documents, all other documents shared more globally are indexed only from the owner's folder, but with the associated permissions, so that who ever is authorized to see the document can find it in Coveo search results.

**Fully supported security model**

The connector fully supports the Google Drive security model using a security provider to get permissions for each indexed item. This means that, in Coveo search interfaces, a user searching Google Drive content only sees the content to which he has access.

**Incremental refresh**

Supports incremental refresh to periodically query Google Drive for the latest edits, keeping the index content up-to-date.

**Out-of-the-box configuration**

The connector is ready to use with minimal configuration to indicate which items to index and which metadata to use.

**Multithreading**

The connector can run multiple threads, which can improve performances considerably (see Modifying Hidden Google Drive for Work Source Parameters).

**Feature History**

<table>
<thead>
<tr>
<th>CES version</th>
<th>Monthly release</th>
<th>Features</th>
</tr>
</thead>
<tbody>
<tr>
<td>7.0.7022+</td>
<td>September 2014</td>
<td>Supports refreshing or deleting from the index a specific folder or document</td>
</tr>
<tr>
<td>7.0.6767</td>
<td>June 2014</td>
<td>Populates syst0 and sysfrom fields allowing to create Shared To and Shared From facets.</td>
</tr>
<tr>
<td>7.0.6684</td>
<td>May 2014</td>
<td>Significant crawling performance improvement and additional source options [more]</td>
</tr>
<tr>
<td>7.0.5556+</td>
<td>June 2013</td>
<td>Beta version introduction</td>
</tr>
</tbody>
</table>

**What's Next?**

Review the steps to deploy the Google Drive for Work connector (see "Google Drive for Work Connector Deployment Overview" on page 1001).

**9.18.3 Google Drive for Work Connector Deployment Overview**

The following procedure outlines the steps needed to deploy the Google Drive for Work connector. The steps indicate the order in which you must perform configuration tasks on both the Google and Coveo servers.
To deploy the Google Drive for Work connector

1. Validate that your environment meets the requirements (see "Google Drive for Work Connector Requirements" on page 1003).

2. On the Google server:
   a. Create a Google API Console project to authorize the Coveo connector to access the Google Drive of your users (see "Authorizing the Coveo Connector to Access Your Google Drive" on page 983).
   b. Modify security parameters in your Google Apps account to grant the connector access to your Google Apps for Work (see "Authorizing the Coveo Connector to Access Your Google Apps for Work" on page 987).

3. On the Coveo server, in the Coveo Administration Tool:
   a. Set up the crawling account
      The Coveo connector needs an account that can list the various drives and users of the domain. This is typically the administrator of the Google Apps domain. There are two methods available to get the permissions from the crawling account depending on your CES version:
      - **CES 7.0.7433+ (February 2015)** The method, that only requires your admin account email, uses the service account email and its PCKS12 private key file, both obtained in step 2a, to impersonate the admin account without having to create a user identity.
      - **CES 7.0.738+ (January 2015)** Create a CES user identity that contains the credentials (username and password) of your domain administrator (see "Adding a User Identity" on page 420).
   b. Optionally create security providers
      When you want to index Google Drive permissions, you must create two security providers to get Google Apps for Work item permissions and resolve and expand groups.
      In Google Drive, users are identified by their email addresses. Consequently, permissions returned by the Google Apps for Work security provider for each document are email addresses. The Google Apps for Work security provider then requires another security provider to uniquely identify users from their email addresses.
      i. Start by selecting or creating an Email or an Active Directory security provider that the Google Apps for Work security provider will use to resolve and expand groups. The security provider type to use depends on how users are authenticated when they access the search interface:
         - When authenticated with their email address, use an Email security provider (see "Configuring an Email Security Provider" on page 65).
         - When authenticated with an Active Directory account, use an Active Directory security provider (see "Configuring an Active Directory Security Provider" on page 1141).
Notes:

- CES comes with an Active Directory security provider that you can configure to connect to the default domain. When your environment contains more than one domain, you can select an Active Directory security provider that you created for other domains.
- An Active Directory security provider is appropriate only when the User Principal Name (UPN) matches the email address for all users.

Note: You may require to also use a REGEX Transform Member Name security provider in between the two other security providers to map member types. Contact Coveo Support for assistance.

9.18.4 Google Drive for Work Connector Requirements

Your environment must meet the following requirements to be able to use the Google Drive for Work connector:

- **CES 7.0.5989+ (October 2013)**
- Coveo license for the Google Drive (Google Apps for Work) connector

  Your Coveo license must include support for the Google Drive for Work connector to be able to use this connector.

- A valid Google Account

  Using a Google Account with administrator privilege, you must log in the Google API Console to authorize Coveo to access the Google Drive of your users (see Authorizing the Coveo Connector to Access Your Google Drive).

- Administrator credentials to your Google Apps account
You must log in to your Google Apps account to modify security options and authorize Coveo to access your Google Apps for Work (see Authorizing the Coveo Connector to Access Your Google Apps for Work).

- Google Drive storage licenses for your Google Apps users
  
  In your Google Apps account, you must activate the Google Drive service (see Authorizing the Coveo Connector to Access Your Google Apps for Work).

- Coveo Master server free disk space for temporary files
  
  Before indexing your Google Drive, ensure that your Coveo Master server has sufficient free hard disk space to temporarily store indexed Google Drive content.

  Starting with the CES 7.0.6547 March 2014 monthly release, the Google Drive connector creates a BLOB store on the Coveo Master server ([CES_Path]\Index\Crawlers\BlobStore or [CES_Path]\Index\Crawlers\BlobStore32) where shared downloaded documents with sizes greater than 100 KB are temporarily saved. This mechanism prevents downloading and re-indexing all copies of shared documents and allows to index metadata associated with each shared document copy.

What’s Next?

Grant Coveo access to the Google Drive of your users by creating a Google API Console project and modifying security options in your Google Apps account (see "Authorizing the Coveo Connector to Access Your Google Drive" on page 983).

9.18.5 Setting Google Permissions (Google for Work)

Before you start configuring the Coveo connector for Google Drive (Google for Work), you must first set appropriate Google permissions.

Refer to the following topics to perform the necessary Google security configuration:

1. "Authorizing the Coveo Connector to Access Your Google Drive" on page 983
2. "Authorizing the Coveo Connector to Access Your Google Apps for Work" on page 987

9.18.6 Configuring a Google Drive for Work Security Provider

The Coveo Google Drive for Work connector fully supports the Google security model. When you want users searching for Google Drive content in a Coveo search interface to only see the content to which they have access in Google Drive, the connector needs a security provider to be able to index the permissions for each indexed Google Drive item.

**Note:** You can get familiar with how Coveo components deal with permissions on documents both at indexing and query time.

To configure a Google Drive for Work security provider

1. On the Coveo server, access the Administration Tool.
3. In the navigation panel on the left, click Security Providers.
4. In the **Security Providers** page, click **Add** to create a new security provider.

5. In the **Modify Security Provider** page:

   ![Security Provider Configuration](image)

   a. Configure the following required parameters:

   **Name**

   Choose a meaningful name to identify the security provider.

   **Example:** Google Drive for Work Security Provider

   **Security Provider Type**

   In the drop-down list, select **Google Apps (x64)**.

   **User Identity**

   In the drop-down list:
**Activate domain-wide mode**

You must select this option when you plan to use this security provider with a **Google Drive (Google Apps)** source type.

**Security Provider**

Select the security provider that you selected or created to allow this security provider to resolve and expand the groups (see **Google Drive for Work Connector Deployment Overview**).

**[Domain-wide mode] Managed domains**

Enter the domain that you want to index. When your Google Apps account contains more than one domain, you can enter a semicolon-separated list of domains to index. The security provider will resolve and expand groups for the specified domain(s).

**Examples:**

- One domain: mysubdomain.mycompany.com
- Multiple domains: myfirstdomain.com;myseconddomain.com

**Important:** The domain(s) specified in this list must match the one(s) specified in the source **Domain (s) list** (see **Configuring and Indexing a Google Drive for Work Source**).

b. **CES 7.0.7433+ (February 2015)** Configure the following required parameters:

**Service Account Email Source**

Enter the service account **Email address** previously obtained (see **Authorizing the Coveo Connector to Access Your Google Drive**).

**Example:** 12345678901@developer.gserviceaccount.com

**Certificate File Path Source**

**Note:** **CES 7.0.7599+ (April 2015)** This parameter is no longer required and can be left empty when you use the **CertificateFileData** hidden parameter (see **CertificateFileData**).

Enter the path on the Coveo Master server where you saved the previously obtained service account's PKCS12 private key file (see **Authorizing the Coveo Connector to Access Your Google Drive**).

**Example:** D:\CES7\Config\1234ab8e315e67a89e02f16ea38bd44d609471ff-privatekey.p12

**Domain Administrator Email Source**

Enter the domain admin account email used to obtain the list of users in the domain.
c. **CES 7.0.7599+ (April 2015)** (Optional) Click **Add Parameter** and then use the following hidden parameter when you let the **Certificate File Path** parameter box empty:

**CertificateFileData**

The service account's PKCS12 private key file data encoded in Base64. The default value is null.

**Notes:**
- You need to open the certificate in a text editor and use an encoding application such as Motobit to convert the certificate content to the Base64 format.
- This parameter is only used when the Certificate File Path parameter box is empty (see **Certificate File Path**).

d. Leave the **Allow Complex Identities** cleared as it does not apply to this type of security provider.

e. Click **Apply Changes**.

What's Next?

Create and index a source (see "Configuring and Indexing a Google Drive for Work Source" on page 1007).

9.18.7 Configuring and Indexing a Google Drive for Work Source

A source defines a set of configuration parameters for a specific Google Apps for Work account.

To configure and index a Google Drive for Work source

1. On the Coveo server, access the Administration Tool.
2. Select **Index > Sources and Collections**.
3. In the **Collections** section:
   a. Select an existing collection in which you want to add the new source.

   OR

   b. Click **Add** to create a new collection.
4. In the **Sources** section, click **Add**.

   The **Add Source** page that appears is organized in three sections.
5. In the **General Settings** section of the **Add Source** page:
a. Enter the appropriate value for the following required parameters:

**Name**

Enter a descriptive name of your choice for the connector source.

**Example:** Google Drive for Work

**Source Type**

Select the connector used by this source. In this case, select **Google Drive (Google Apps)**.

**Notes:**

- If you do not see **Google Drive (Google Apps)**, your environment does not meet the requirements (see "Google Drive for Work Connector Requirements" on page 1003).
- Do not select the **Google Drive (Single User)** option.

**Addresses**

This parameter is not used, but must not be empty. Enter **http://www.google.com**.

**Fields**

Select the field set that you created for your Google Drive source (see **Google Drive for Work Connector Deployment Overview**).

**Refresh Schedule**

Time interval at which the index is automatically refreshed to keep the index content up-to-date. By
default, the Every day option instructs CES to refresh the source everyday at 12 AM. Because the incremental refresh takes care of maintaining the source up-to-date, you can select a longer interval such as Every Sunday.

b. Review the value for the following parameters that often do not need to be modified:

**Rating**

Change this value only when you want to globally change the rating associated with all items in this source relative to the rating to other sources.

**Example:** When a source replaces a legacy system, you may want to set this parameter to High, so that in the search interface, results from this source appear earlier in the list compared to those from legacy system sources.

**Document Types**

If you defined a custom document type set for this source, select it.

**Active Languages**

If you defined custom active language sets, ensure to select the most appropriate for this source.

6. In the **Specific Connector Parameters & Options** section of the **Add Source** page:

   a. In the **Mapping File** box, optionally enter the path to a mapping file that should apply to the items in this source.

      Leave this box empty to use the default mapping that should be appropriate in most cases.

      When the default mapping does not fulfill your needs, contact Coveo Support for assistance. Your XML mapping file must respect the standard Coveo mapping file schema.
b. **Domain Admin e-mail**

   Enter the domain admin account email used to obtain the list of users in the domain.

   **Example:** admin@domain.com

   **Note:** The e-mail you enter here must be the same as the one you entered previously when configuring the security provider (see Configuring a Google Drive for Work Security Provider).

c. **Domain(s)**

   Using the following parameters, authorize the Coveo crawler to access the Google Drive of your users:

   **Domain(s)**

   Enter the Google Drive domain that you want to index. When your Google Apps account contains more than one domain, you can enter a semicolon-separated list of domains to index.

   **Examples:**
   - One domain: mydomain.com
   - Multiple domains: myfirstdomain.com;my.second.domain.com

   **Important:** The domain(s) specified in this list must match the one(s) specified in the security provider [Domain-wide mode] Managed domains list (see Configuring a Google Drive for Work Security Provider).

   **Service account e-mail**

   Enter the service account Email address previously obtained (see Authorizing the Coveo Connector to Access Your Google Drive). It must be the same email that you entered when configuring the security provider (see Configuring a Google Drive for Work Security Provider).

   **Example:** 12345678901@developer.gserviceaccount.com

   **Service account PCKS12 file path**

   **Note:** This parameter is no longer required and can be left empty when you use the ServiceAccountPcks12FileData hidden parameter (see Modifying Hidden Google Drive for Work Source Parameters).

   Enter the path on the Coveo Master server where you saved the previously obtained service account's PCKS12 private key file (see Authorizing the Coveo Connector to Access Your Google Drive). It must be the same path that you entered when configuring the security provider (see Configuring a Google Drive for Work Security Provider).

   **Example:** D:\CES7\Config\1234ab8e315e67a898e02f16ea38bd44d609471ff-privatekey.p12

d. **Select the type of content to index using the following options:**
Crawl trashed items

Select to index the items in the user's trash. Not selected by default.

Crawl custom properties

Select to index custom properties that Google applications or your custom applications added on items. Not selected by default.

Note: Crawling custom properties adds one API call per indexed document. Selecting this option can notably increase the number of calls to the Google Drive API and the crawling time.

Index Users CES 7.0.9167+ (December 2017)

Select to index Google Drive users as separate documents. Not selected by default.

e. Click Add Parameter when you want to show and change the value of advanced source parameters (see "Modifying Hidden Google Drive for Work Source Parameters" on page 1013).

f. The Option check boxes generally do not need to be changed:

Index Subfolders

This parameter is not taken into account for this connector.

Index the document's metadata

When selected, CES indexes all the document metadata, even metadata that are not associated with a field. The orphan metadata are added to the body of the document so that they can be searched using free text queries.

When cleared (default), only the values of system and custom fields that have the Free Text Queries attribute selected will be searchable without using a field query.

Example: A document has two metadata:

- LastEditedBy containing the value Hector Smith
- Department containing the value RH

In CES, the custom field CorpDepartment is bound to the metadata Department and its Free Text Queries attribute is selected.

When the Index the document's metadata option is cleared, searching for RH returns the document because a field is indexing this value. Searching for hector does not return the document because no field is indexing this value.

When the Index the document's metadata option is selected, searching for hector also returns the document because CES indexed orphan metadata.

Document's addresses are case-sensitive

Ensure that this option is selected because Google Drive document IDs are case sensitive.
Generate a cached HTML version of indexed documents

When you select this check box (recommended), at indexing time, CES creates HTML versions of indexed documents. In the search interfaces, users can then more rapidly review the content by clicking the Quick View link rather than opening the original document with the original application. Consider clearing this check box only when you do not want to use Quick View links or to save resources when building the source.

Open results with cached version

Leave this check box cleared (recommended) so that in the search interfaces, the main search result link opens the original document with the original application. Consider selecting this check box only when you do not want users to be able to open the original document but only see the HTML version of the document as a Quick View. In this case, you must also select Generate a cached HTML version of indexed documents.

7. In the Security section of the Add Source page:

(a) When you chose to index Google Drive permissions, in the Security Provider drop-down list, select the Google Drive for Work security provider that you created for this source (see "Configuring a Google Drive for Work Security Provider" on page 1004).

(b) In the Authentication drop-down list:
   - CES 7.0.7433+ (February 2015) Select (none).
   - CES 7.0.7338–(January 2015) Select the user identity that you created for this source (see Google Drive for Work Connector Deployment Overview).

8. Click Save to save the source configuration.

9. When you chose to not index Google Drive permissions, you can set source level permissions that apply to all documents in the source:

(a) In the navigation panel on the left, click Permissions.

(b) In the Permissions page, select Specify the security permissions to index.

(c) In the Allowed Users and Denied Users boxes, enter the users and groups that you respectively want to allow or deny to see search results from this source. The default is to allow everyone \$-1-1-0\ (Active
10. When you are ready to start indexing the Google Drive source, click Rebuild.

11. Validate that the source building process is executed without errors:
   - In the navigation panel on the left, click Status, and then validate that the indexing proceeds without errors.
   - OR
   - Open the CES Console to monitor the source building activities.

What's Next?

Set an incremental refresh schedule for your source.

Consider modifying some hidden source parameters to try resolving other issues (see "Modifying Hidden Google Drive for Work Source Parameters" on page 1013).

9.18.8 Modifying Hidden Google Drive for Work Source Parameters

The Add Source and Source: ... General pages of the Administration Tool present the parameters with which you can configure the connector for most Google Drive for Work setups. More advanced and more rarely used parameters are hidden. You can choose to make one or more of these parameters appear in the Add Source and Source: ... General pages of the Administration Tool so that you can change their default value. Consider changing values of hidden parameters when you encounter issues.

The following list describes the advanced hidden parameters available with Google Drive for Work sources. The parameter type (integer, string, etc.) appears between parentheses following the parameter name.

IgnoreLinkRequiredPermissions (Boolean) CES 7.0.8225.5+ (Mars 2016)

Whether to ignore permissions with a required link on the documents. The default value is true.

Notes:

- Permissions requiring links are either "Anyone with the link" or "Anyone at <domain> with the link" (see Share Google Drive files and folders).
- By default, in a Coveo search page, end-users cannot find Google Drive documents in search results with either the "Anyone with the link" or "Anyone at <domain> with the link" permissions.

NumberOfRefreshThreads (Integer)

The number of refresh threads used by the crawler for this source. The default value is 8.

ResultsPerPage (Integer) CES 7.0.6684+ (May 2014)

Number of results to fetch per request made to Google Drive. The default value is 100. The minimum value is 1 and the maximum value is 1000. A small value (not recommended) forces the connector to make small but frequent queries to Google Drive. A larger value (recommended) leads to larger and less frequent queries.
**Note:** Queries to the Google Drive service are made per folder.

**Example:** With a value of 100, if a folder contains 180 items, two queries will be necessary to obtain the items.

**CommentsPerPage (Integer)** CES 7.0.6684+ (May 2014)

Number of comments to fetch per request made to Google Drive. The default and maximum value is 100. The minimum value is 1.

**CrawlSharedWithMeItems (Boolean)** CES 7.0.6684+ (May 2014)

Whether to process items that have been shared with each user (Shared with me). The default value is true.

**CrawlComments (Boolean)** CES 7.0.6684+ (May 2014)

Whether to index comments from each item. The default value is false. Consider setting this parameter to true when you must have searchable comments. However, make comments searchable costs API calls and can increase crawling time depending on the number of comments in your Google Drive content.

**Note:** CES 7.0.6942- (August 2014) The CrawlComments hidden parameter default value is true.

**UseFolderLinksInMyDrive (Boolean)** CES 7.0.6684+ (May 2014)

Whether to use folder links that open directly in My Drive rather than in a folder view. The default value is true.

**Example:** In the search results breadcrumb for a Shared with me document, when a user clicks the parent folder and this parameter is set to false, the opened URL is in the form https://drive.google.com/a/mydomain.com/folderview?id=[GUID]&usp=drive-sdk#, showing a file and folder view with a Open in My Drive link.

When set to true, the opened URL is in the form https://drive.google.com/a/mydomain.com/?usp=folder#folders/[GUID], directly opening in My Drive, as if the user had clicked the Open in My Drive link, thus saving one click.

**IndexGoogleAppsDocThumbnails (Boolean)**

Whether to index thumbnails for Google Apps for Work documents. The default value is false. Setting this parameter to true to index document thumbnails would increase the crawling time by about 5%.

**IndexNativeDocThumbnails (Boolean)**

Whether to index thumbnails for native documents (PDF, DOC, XLS, etc.). The default value is false.

**AddFromAndToFields (Boolean)** CES 7.0.7022+ (September 2014)

Whether to add the sysfrom and systo fields to system fields. The default value is true. Adding these fields can have a significant impact on the crawling performance, so consider setting this parameter to false to improve crawling performance.

**EnablePrefetcher (Boolean)** CES 7.0.7104+ (October 2014)

Whether the prefetcher is used by the crawler. The default value is false in which case the connector
processes the items of a folder retrieved with an API call before making the next API call for the next Google Drive folder.

It is recommended to enable the prefetcher that immediately makes the next API call and improves crawling performances, particularly when folders contain many documents.

**NumberOfPrefetchedItems (Integer)** CES 7.0.7104+ (October 2014)

The maximum number of items to prefetch will save in memory when the prefetcher is enabled (see EnablePrefetcher). The default value is 300. The minimum value is 1 and the maximum value is 1000.

Consider increasing the **NumberOfPrefetchedItems value** if you increase the number of threads used by the crawler (see "**NumberOfRefreshThreads (Integer)**" on page 1013).

**ServiceAccountPkcs12FileData (Integer)** CES 7.0.7599+ (April 2015)

The service account's PKCS12 private key file encoded data. The PKCS12 file encoded in Base64. The default value is null.

**Notes:**
- You need to open the certificate in a text editor and use an encoding application such as Motobit to convert the certificate content to the Base64 format.
- This parameter is only used when the Service account PKCS12 file path parameter is empty (see Configuring and Indexing a Google Drive for Work Source).

**FileMimeTypesWithComments (String)** CES 7.0.7914+ (October 2015)

Semicolon separated list of document MIME types which support comments in Google Drive (see Supported MIME Types). The default value is application/vnd.google-apps.document;application/vnd.google-apps.presentation;application/vnd.google-apps.spreadsheet;application/vnd.google-apps.drawing.

To modify hidden Google Drive for Work source parameters

1. Refer to "Adding an Explicit Connector Parameter" on page 450 to add one or more Google Drive for Work source parameters.

2. For a new Google Drive for Work source, access the Add Source page of the Administration Tool to modify the value of the newly added advanced parameter:
   a. Select Index > Sources and Collections.
   b. Under Collections, select the collection in which you want to add the source.
   c. Under Sources, click Add.
   d. In the Add Source page, edit the newly added advanced parameter value.

3. For an existing Google Drive for Work source, access the Source: ... General page of the Administration Tool to modify the value of the newly added advanced parameter:
a. Select Index > Sources and Collections.

b. Under Collections, select the collection containing the source you want to modify.

c. Under Sources, click the existing Google Drive for Work source in which you want to modify the newly added advanced parameter.

d. In the Source: ... General page, edit the newly added advanced parameter value.

4. Rebuild your Google Drive for Work source to apply the changes to the parameters.

9.19 Google Sites Connector

The Coveo beta connector for Google Sites allows Coveo administrators to index and integrate the content of one or more domain or private Google Sites into the Coveo unified index so that in the Coveo search interfaces, a user can easily find content to which he has access in Google Sites.

9.19.1 Features

The Google Sites connector features are:

Content indexing

The connector can index Google Sites content from either a single user Google Account or a Google Apps domain.

The connector can index the following Google Sites content type to make it searchable by end-users:

- Web pages
- Attachments
- Announcements (Announcement pages)
- Files and web attachments (File cabinets)
- List items (List pages)

Note: The comments cannot be indexed because the current Google Sites API only allows to access comments created with the old commenting systems, not those created with the new commenting system.

Site-level permission indexing

The connector can index the Google Sites site-level permissions for each item. This means that, in Coveo search interfaces, a user searching Google Sites content only sees the content to which he has access as specified in site-level permissions.

Note: The connector cannot index page-level permissions because this information is not available through the Google Sites API. This means that a user that is denied access to a specific Google Sites page could see this page in Coveo search results.
Incremental refresh

Supports incremental refresh to periodically query Google Sites for the latest edits, keeping the index content up-to-date.

**Note:** The incremental refresh has the following limitations:

- Permission changes alone cannot be detected.
- Does not work when the last refresh date is more than 30 days, because list of deleted items are only kept for 30 days.

Multithreading

The connector can run multiple threads, which can improve performances considerably.

Feature History

<table>
<thead>
<tr>
<th>CES version</th>
<th>Monthly release</th>
<th>Features</th>
</tr>
</thead>
<tbody>
<tr>
<td>7.0.7183+</td>
<td>November 2014</td>
<td>Connector provides default field set and mapping file [more]</td>
</tr>
<tr>
<td>7.0.6225+</td>
<td>December 2013</td>
<td>Connector introduction (Beta)</td>
</tr>
</tbody>
</table>

What's Next?

Review the steps to deploy the Google Sites connector (see "Google Sites Connector Deployment Overview" on page 1017).

9.19.2 Google Sites Connector Deployment Overview

The following procedure outlines the steps needed to deploy the Google Sites connector. The steps indicate the order in which you must perform configuration tasks on both the Google and Coveo servers.

To deploy the Google Sites connector

1. Validate that your environment meets the requirements (see "Google Sites Connector Requirements" on page 1019).

2. On the Google console, authorize the Coveo connector to access your Google Sites.

   You must create a Google API Console project to grant the connector access to the Google Sites that you want to index (see "Granting the Connector Access to Your Google Sites" on page 1020).

3. On the Coveo server, in the Coveo Administration Tool:

   a. Configure a user identity

   The Coveo connector needs an account to crawl your Google Sites content. For this purpose, select an existing Google Apps account or create a new one. When you want to index permissions, the crawling account must have administrator rights because ACL Feed access is required. When you do not want to
index permissions, an account that has read only permissions to the whole content that you want to index is sufficient.

Create a CES user identity that contains the credentials of your Google Apps crawling account (see "Adding a User Identity" on page 420).

b. Optionally create security providers

When you want to index Google Sites site-level permissions, you must create two security providers to get permissions and, resolve and expand groups.

In Google Sites, users are identified by their email addresses. Consequently, permissions returned by the Google Apps security provider for each document are email addresses. The Google Apps security provider then requires another security provider to uniquely identify users from their email addresses.

i. Start by selecting or creating an Email or an Active Directory security provider that the Google Apps security provider will use to resolve and expand groups. The security provider type to use depends on how users are authenticated when they access the search interface:

- When authenticated with their email address, use an Email security provider with no user identity (see "Configuring an Email Security Provider" on page 65).
- When authenticated with an Active Directory account, use an Active Directory security provider (see "Configuring an Active Directory Security Provider" on page 1141).

Notes:

- An Active Directory security provider is appropriate only when the User Principal Name (UPN) matches the email address for all users.
- CES comes with an Active Directory security provider that you can configure to connect to the default domain. When your environment contains more than one domain, you can select an Active Directory security provider that you created for other domains.

ii. Create a Google Apps security provider that the connector uses to resolve indexed permissions (see "Configuring a Google Sites Security Provider" on page 1022).

c. CES 7.0.7104—(October 2014) Optionally, when you want to index Google Sites metadata, create a custom mapping file.

A sample mapping file defines a few custom Google Sites field that can be used to create a rich Google Sites search interface, for example, providing more specific facets (see "Creating a Custom Google Sites Connector Mapping File" on page 1024).

Note: CES 7.0.7183+ (November 2014) The Google Sites connector comes with a default mapping file (see Configuring and Indexing a Google Sites Source).

d. Create a Google Sites field set to take advantage of the available Google Sites metadata.

It is recommended to start by importing the default Google Sites field set file ([CES_Path]\Bin\Coveo.CES.CustomCrawlers.GoogleSites.FieldSet.xml to be able to easily add Google Sites specific facets to your Coveo search interfaces.

www.coveo.com
**Note**: CES 7.0.7104– (October 2014) It is recommended to download the zipped Google Sites sample Field set XML file, and import it in CES.

The sample Google Sites field set defines the custom fields that match the custom fields defined in the sample mapping file.

e. Configure and index a Google Sites source.

The connector must know details about the authorized access to the Google Sites of your users to index its content (see "Configuring and Indexing a Google Sites Source" on page 1026).

f. If you encounter issues, verify if modifying the default value of hidden source parameters can help resolve the problems (see "Modifying Hidden Google Sites Source Parameters" on page 1032).

### 9.19.3 Google Sites Connector Requirements

Your environment must meet the following requirements to be able to use the Google Sites connector:

- CES 7.0.6225+ (December 2013)
- Coveo license for the Google Sites connector
Your Coveo license must include support for the Google Sites connector to be able to use this connector.

- A valid Google Account

  Using a Google Account with administrator privilege, you must log in the Google API Console to authorize the Coveo connector to access your Google Sites (see Granting the Connector Access to Your Google Sites).

What’s Next?

Grant Coveo access to your Google Sites (see Granting the Connector Access to Your Google Sites).

9.19.4 Granting the Connector Access to Your Google Sites

Before you can configure Google Sites sources, you must grant the Connector access to the Google Sites content to index. The steps are the same whether you are authorizing access to Google Sites associated to a personal Google account or a Google Apps domain account.

A Coveo source needs to know the values for the Client ID, Client Secret, and OAuth2 Refresh Token associated with your Google Sites.

9.19.4.1 Getting Google Sites Client ID and Client Secret values

1. Go to the Google Developers Console, and log in using a Google Account with administrator credentials.

2. At the left of the Filter by name, ID or label input, click the drop-down menu, and then select the organization in which you want to create the Google Developer Console project.

3. Create an API project for the Coveo connector (CES 7) or source (Coveo Cloud):
   a. In the Manage resources panel, click Create a project.
   b. (When your project limit is exceeded) In the Increase Project Limit page, click Request increase, and then complete the form.
   c. In the New Project dialog page, enter the project required information.
i. Enter a **Project name**.

   **Note:** The project ID is automatically created based on the project name. You can always modify the project ID by clicking **Edit**.

ii. (When you create the first project in your organization only) Answer the **Please email me updates regarding feature announcements, performance suggestions, feedback surveys and special offers.** question using the **Yes** or **No** checkbox.

iii. (When you create the first project in your organization only) After you **have read and agree to the Google Play Android Developer API Terms of Service**, click the **Yes** check box.

iv. Click **Create**.

4. Create a Client ID for the Coveo connector.

   a. In the sidebar on the left, select **Credentials**.

   b. In the **Credentials** page, click the **Create credentials** drop-down list menu, and then select **OAuth client ID**.

   c. In the **Create client ID** dialog box:
      
      a. Under **Application type**, click the **Other** checkbox.

      b. In the box, enter an application **Name**.

      c. Click **Create**.

5. In the **OAuth client** dialog box that appears, note the **Client ID** and **Client secret** values.
9.19.4.2 Getting a Google Sites OAuth2 Refresh Token

Now that the Google Sites Connector is registered by creating an API Project and obtained its OAuth2 Client ID, you need to get authorization for the Connector to actually access the Google Sites content.

The Coveo connector needs an OAuth2 refresh token that can only be obtained programmatically (see Using OAuth 2.0 to Access Google APIs).

If you do not have a tool to retrieve the OAuth2 refresh token, contact Coveo Support for assistance.

9.19.5 Configuring a Google Sites Security Provider

The Coveo Google Sites connector supports the Google Sites site-level permissions.

When you want users searching for Google Sites content in a Coveo search interface to only see the content to which they have access in Google Sites, the connector needs a security provider to be able to index the permissions for each indexed Google Sites item.

**Note:** You can get familiar with how Coveo components deal with permissions on documents both at indexing and query time.

To configure a Google Drive for Work security provider

1. On the Coveo server, access the Administration Tool.
2. Select **Configuration > Security**.
3. In the navigation panel on the left, click **Security Providers**.
4. In the **Security Providers** page, click **Add** to create a new security provider.
5. In the **Modify Security Provider** page:
a. Configure the following required parameters:

**Name**

Choose a meaningful name to identify the security provider.

**Example:** When the security provider is to be used by a source indexing Google Sites associated with an Apps domain, you can enter Google Sites Apps Domain Security Provider.

**Security Provider Type**

In the drop-down list, select **Google Apps (x64)**.

**User Identity**

In the drop-down list, select the user identity that you selected or created previously (see Google Sites Connector Deployment Overview).

**Activate domain-wide mode**

You must select this option when you plan to use this security provider with a **Google Sites** source that indexes a Google Sites for an Apps domain.

Clear this option when the security provider is for a source indexing Google Sites of an individual user.
Security Provider

Select the security provider that you selected or created to allow this security provider to resolve and expand the groups (see Google Sites Connector Deployment Overview).

[Domain-wide mode] Managed domains

Enter the domain that you want to index. When your Google Apps account contains more than one domain, you can enter a semicolon-separated list of domains to index. The security provider will resolve and expand groups for the specified domain(s).

Examples:

- One domain: mydomain.com
- Multiple domains: myfirstdomain.com;my.second.domain.com

Important: The domain(s) specified in this list must match the one(s) specified in the Addresses box of the source that will use this security provider (see Configuring and Indexing a Google Sites Source).

Allow Complex Identities

Leave this option cleared as it does not apply to Google Sites.

b. Click Apply Changes.

What's Next?

Create and index a source (see Configuring and Indexing a Google Sites Source).

9.19.6 Creating a Custom Google Sites Connector Mapping File

The Google Sites connector comes with a default mapping file (CES 7.0.7183+ (November 2014)) which allows to index the retrieved Google Sites default metadata. However, when you want to modify the default behavior of the Google Sites connector, creating a custom mapping file is required.

The following table presents Google Sites metadata retrieved by the connector. Metadata prefixed with coveo_ are extra metadata created by the Coveo connector.

Note: CES 7.0.7183+ (November 2014) Metadata prefixed with coveo_ and other absent metadata from the default mapping file are contained in the default field set ([CES_Path]\Bin\Coveo.CES.CustomCrawlers.GoogleSites.FieldSet.xml).

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>coveo_id</td>
<td>String</td>
<td>Item unique identifier</td>
</tr>
<tr>
<td>coveo_parent_id</td>
<td>String</td>
<td>Parent item unique identifier</td>
</tr>
<tr>
<td>coveo_domain_name</td>
<td>String</td>
<td>The domain name of the Google Site that contains this item.</td>
</tr>
<tr>
<td>Name</td>
<td>Type</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------</td>
<td>--------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>coveo_site_name</td>
<td>String</td>
<td>The site name of the Google Site that contains this item.</td>
</tr>
<tr>
<td>coveo_item_type</td>
<td>String</td>
<td>Item type formatted ready to be displayed.</td>
</tr>
<tr>
<td>title</td>
<td>String</td>
<td>Item title</td>
</tr>
<tr>
<td>alternate_url</td>
<td>String</td>
<td>Item alternate URI (clickable link to the page or item in Google Sites)</td>
</tr>
<tr>
<td>clickable_link</td>
<td>String</td>
<td>Item clickable link</td>
</tr>
<tr>
<td>is_draft</td>
<td>Boolean</td>
<td>Indicates if the item is in draft state or not.</td>
</tr>
<tr>
<td>kind</td>
<td>String</td>
<td>Item kind (item type)</td>
</tr>
<tr>
<td>folder</td>
<td>String</td>
<td>Item folder name (if any)</td>
</tr>
<tr>
<td>categories</td>
<td>String</td>
<td>Item categories (tags)</td>
</tr>
<tr>
<td>summary</td>
<td>String</td>
<td>Item summary</td>
</tr>
<tr>
<td>edited</td>
<td>DateTime</td>
<td>Item edited date and time</td>
</tr>
<tr>
<td>published</td>
<td>DateTime</td>
<td>Item published date and time</td>
</tr>
<tr>
<td>updated</td>
<td>DateTime</td>
<td>Item updated date and time</td>
</tr>
<tr>
<td>author_names</td>
<td>String</td>
<td>Item author names</td>
</tr>
<tr>
<td>author_emails</td>
<td>String</td>
<td>Item author emails</td>
</tr>
<tr>
<td>content_source</td>
<td>String</td>
<td>Item content source (link pointing to the attachment or web attachment)</td>
</tr>
<tr>
<td>page_name</td>
<td>String</td>
<td>Item page name in the URL</td>
</tr>
<tr>
<td>revision</td>
<td>Integer</td>
<td>Item current revision number</td>
</tr>
</tbody>
</table>

**Note:** CES 7.0.7104—(October 2014) When you want to index Google Sites metadata, you must create a custom mapping file that will be used by your Google Sites source. The mapping file specifies which Google Sites metadata will be mapped to which Coveo index custom fields.

Below is a sample Google Sites mapping file with useful mappings for Google Sites metadata.

```xml
<?xml version="1.0" encoding="utf-8" ?>
<Mappings>
  <Version>1</Version>
  <CommonMapping>
    <Fields>
      <!-- Google Sites custom fields -->
      <Field name="sitedomainname">%{coveo_domain_name}</Field>
      <Field name="siteitemtype">%{coveo_item_type}</Field>
      <Field name="sitename">%{coveo_site_name}</Field>
      <Field name="siteauthoremails">%{author_emails}</Field>
      <Field name="sitekind">%{kind}</Field>
    </Fields>
  </CommonMapping>
</Mappings>
```
To create a custom Google Sites connector mapping file

1. Copy the content of the sample mapping file.

2. Using a text editor:
   a. Edit the file to include the desired Google Site metadata mapping to custom index fields.
   b. Ensure that your custom mapping file respects the standard mapping file format.
   c. Save the file.

3. Copy your custom mapping file on the Coveo Master server in a folder accessible to CES.

   **Example:** Copy the mapping file to `D:\CES7\Config\MyGoogleSitesMappingFile.xml`

What's Next?

Consider using the sample Google Sites field set (see Google Sites Connector Deployment Overview).

Ensure that all the Coveo fields included in your mapping file are created in the index.

9.19.7 Configuring and Indexing a Google Sites Source

A source defines a set of configuration parameters for one or more Google Sites for one Google Apps account.
Note: Create separate Google Sites sources when:

- You have more than one Google apps account to manage your Google Sites domains.
- One source Google Sites associated with a private Google account.

To configure and index a Google Sites source:

1. On the Coveo server, access the Administration Tool.
2. Select Index > Sources and Collections.
3. In the Collections section:
   a. Select an existing collection in which you want to add the new source.
   
   OR

   b. Click Add to create a new collection.
4. In the Sources section, click Add.

   The Add Source page that appears is organized in three sections.

5. In the General Settings section of the Add Source page:
a. Enter the appropriate value for the following required parameters:

**Name**

Enter a descriptive name of your choice for the connector source.

**Example:** Google Sites

**Source Type**

Select the connector used by this source. In this case, select Google Sites.

**Note:** If you do not see Google Sites, your environment does not meet the requirements (see "Google Sites Connector Requirements" on page 1019).

**Addresses**

Enter the address of one or more specific Google Sites in one of the following formats:

- For a private account: https://sites.google.com/site/<my_site>
- For a domain account: https://sites.google.com/a/<my_domain>/<my_site>

**OR**

Enter a starting address to use auto-discovery to crawl all sites accessible to the connector using one of the following formats:

- For a private account: https://sites.google.com/site
- For a domain account: https://sites.google.com/a/<my_domain>

**Notes:**

- The Google Sites returned by the auto-discovery feature are the ones to which the connector was granted access to when the OAuth2 refresh token was generated.
- Only auto-discovery of all accessible sites within a single domain is supported, not for all domains of a specific Google Apps account.
- The auto-discovery only returns sites with sharing permissions explicitly allowing the crawling user; it does not return sites allowing everyone from the domain nor does it consider administrator permissions which grants access to all web sites of the Google App domain.

**Fields**

Select the field set that you created earlier (see Google Sites Connector Deployment Overview).

**Refresh Schedule**

Time interval at which the index is automatically refreshed to keep the index content up-to-date. By default, the **Every day** option instructs CES to refresh the source everyday at 12 AM. Because the incremental refresh takes care of maintaining the source up-to-date, you can select a longer interval such as **Every Sunday**.

b. Review the value for the following parameters that often do not need to be modified:
Rating

Change this value only when you want to globally change the rating associated with all items in this source relative to the rating to other sources.

**Example:** When a source replaces a legacy system, you may want to set this parameter to **High**, so that in the search interface, results from this source appear earlier in the list compared to those from legacy system sources.

Document Types

If you defined a custom document type set for this source, select it.

Active Languages

If you defined custom active language sets, ensure to select the most appropriate for this source.

6. In the **Specific Connector Parameters & Options** section of the **Add Source** page:

   ![Specific Connector Parameters & Options](image)

   a. In the **Mapping File** box, the path to the default mapping file that defines how the connector handles metadata often does not need to be changed.
Notes:

- **CES 7.0.7256– (December 2014)** Enter the path to the default mapping file that defines how the connector handles metadata. You can leave this box empty, in which case no Google Sites metadata will be indexed.
  
  **Example:** D:\Program Files\Coveo Enterprise Search 7\Bin\Coveo.CES.CustomCrawlers.GoogleSites.MappingFile.xml

- **CES 7.0.7104– (October 2014)** If you create a custom mapping file, enter the path where you saved your file on the Coveo server (see "Creating a Custom Google Sites Connector Mapping File" on page 1024). You can leave this box empty, in which case no Google Sites metadata will be indexed.
  
  **Example:** D:\CES7\Config\MyGoogleSitesMappingFile.xml

b. Using the following parameters, authorize the Coveo crawler to access the Google Sites:

**Client's id**

Enter the Client ID value that you got earlier (see "Getting Google Sites Client ID and Client Secret values" on page 1020).

**Client's secret**

Enter the Client Secret value that you got earlier (see "Getting Google Sites Client ID and Client Secret values" on page 1020).

**Client's refresh token**

Enter the OAuth2 refresh token value that you got earlier (see "Getting a Google Sites OAuth2 Refresh Token" on page 1022).

c. Click **Add Parameter** when you want to show and change the value of advanced source parameters (see "Modifying Hidden Google Sites Source Parameters" on page 1032).

d. The **Option** check boxes generally do not need to be changed:

**Index Subfolders**

This parameter is not taken into account for this connector.

**Index the document's metadata**

When selected, CES indexes all the document metadata, even metadata that are not associated with a field. The orphan metadata are added to the body of the document so that they can be searched using free text queries.

When cleared (default), only the values of system and custom fields that have the **Free Text Queries** attribute selected will be searchable without using a field query.
Example: A document has two metadata:

- LastEditedBy containing the value Hector Smith
- Department containing the value RH

In CES, the custom field CorpDepartment is bound to the metadata Department and its Free Text Queries attribute is selected.

When the Index the document's metadata option is cleared, searching for RH returns the document because a field is indexing this value. Searching for hector does not return the document because no field is indexing this value.

When the Index the document's metadata option is selected, searching for hector also returns the document because CES indexed orphan metadata.

Document's addresses are case-sensitive

Leave the check box cleared. This parameter needs to be checked only in rare cases for systems in which distinct documents may have the same name but different casing.

Generate a cached HTML version of indexed documents

When you select this check box (recommended), at indexing time, CES creates HTML versions of indexed documents. In the search interfaces, users can then more rapidly review the content by clicking the Quick View link rather than opening the original document with the original application. Consider clearing this check box only when you do not want to use Quick View links or to save resources when building the source.

Open results with cached version

Leave this check box cleared (recommended) so that in the search interfaces, the main search result link opens the original document with the original application. Consider selecting this check box only when you do not want users to be able to open the original document but only see the HTML version of the document as a Quick View. In this case, you must also select Generate a cached HTML version of indexed documents.

7. In the Security section of the Add Source page:
a. When you chose to index Google Sites permissions, in the Security Provider drop-down list, select the Google Sites security provider that you created for this source (see "Configuring a Google Sites Security Provider" on page 1022).

b. In the User Identity drop-down list, select the user identity that you created for this source (see Google Sites Connector Deployment Overview).

8. Click Save to save the source configuration.

9. When you chose to not index Google Sites permissions, you can set source level permissions that apply to all documents in the source:

a. In the navigation panel on the left, click Permissions.

b. In the Permissions page, select Specify the security permissions to index.

c. In the Allowed Users and Denied Users boxes, enter the users and groups that you respectively want to allow or deny to see search results from this source. The default is to allow everyone (Active Directory Group).

d. Click Apply Changes.

10. When you are ready to start indexing the Google Sites source, click Rebuild.

11. Validate that the source building process is executed without errors:

   - In the navigation panel on the left, click Status, and then validate that the indexing proceeds without errors.

   OR

   - Open the CES Console to monitor the source building activities.

What's Next?

Set an incremental refresh schedule for your source.

Consider modifying some hidden source parameters to try resolving issues (see "Modifying Hidden Google Sites Source Parameters" on page 1032).

9.19.8 Modifying Hidden Google Sites Source Parameters

The Add Source and Source: ... General pages of the Administration Tool present the parameters with which you can configure the connector for most Google Sites setups. More advanced and more rarely used parameters are hidden. You can choose to make one or more of these parameters appear in the Add Source and Source: ... General pages of the Administration Tool so that you can change their default value. Consider changing values of hidden parameters when you encounter issues.

The following list describes the advanced hidden parameters available with Google Sites sources. The parameter type (integer, string, etc.) appears between parentheses following the parameter name.

ResultsPerPage (Integer)

Number of items to fetch per request made to Google Sites. The default value is 100. The minimum value is 1. A
small value (not recommended) forces the connector to make small but frequent queries to Google Sites. A larger value (recommended) leads to larger and less frequent queries.

**NumberofRetries (Integer)**

This parameter determines the number retries allowed when a recoverable call to Google Sites API fails. The default value is 2.

To modify hidden Google Sites source parameters

1. Refer to "Adding an Explicit Connector Parameter" on page 450 to add one or more Google Sites source parameters.
2. For a new Google Sites source, access the **Add Source** page of the Administration Tool to modify the value of the newly added advanced parameter:
   a. Select **Index > Sources and Collections**.
   b. Under **Collections**, select the collection in which you want to add the source.
   c. Under **Sources**, click **Add**.
   d. In the **Add Source** page, edit the newly added advanced parameter value.
3. For an existing Google Sites source, access the **Source: ... General** page of the Administration Tool to modify the value of the newly added advanced parameter:
   a. Select **Index > Sources and Collections**.
   b. Under **Collections**, select the collection containing the source you want to modify.
   c. Under **Sources**, click the existing Google Sites source in which you want to modify the newly added advanced parameter.
   d. In the **Source: ... General** page, edit the newly added advanced parameter value.
4. Rebuild your Google Sites source to apply the changes to the parameters.

### 9.20 IBM Notes Connector

**Deprecated**

The Coveo IBM Notes (formerly known as Lotus Notes) connector allows a Coveo administrator to bring the content of IBM Notes databases into the unified index so that it becomes searchable by end-users.

**Note:** As of March 2, 2017, the IBM Notes connector is deprecated (see "What Does Deprecated Mean for a Coveo Connector?" on page 739).

### 9.20.1 Features

**Content Indexing**

The connector can index all IBM Notes database content such as:
- Emails
- Address books
- Document library
- Documents
- Metadata
- Attachments
- OLE objects

Security

Security permissions on IBM Notes items are indexed and can be fully mapped to their corresponding Windows permissions (see "About the Notes Security Mapping File" on page 1036).

Incremental Refresh

Updated documents in a database (content/security) are periodically re-indexed by the connector (see Configuring and Indexing an IBM Notes Source).

Pause/Resume

When indexing IBM Notes databases, the connector can be paused and resumed.

Miscellaneous

- All databases under a common folder can be indexed using a single address (see Configuring and Indexing an IBM Notes Source).
- Metadata mappings can be fully customized (mapping of IBM Notes fields to CES fields).
- Search results can redirect users to the original documents, which are directly in the IBM Notes Client.

What's Next?

Review the deployment process for the IBM Notes connector (see "IBM Notes Connector Deployment Overview" on page 1034).

9.20.2 IBM Notes Connector Deployment Overview

The following procedure outlines the steps needed to deploy the IBM Notes connector. The steps indicate the order in which you must perform configuration tasks on both IBM Notes (Domino) and Coveo servers.

To deploy the IBM Notes connector

1. Validate that your environment meets the requirements (see "IBM Notes Connector Requirements" on page 1035).
2. Once IBM Notes Client is configured, open one database (which has the .nsf extension) stored on the targeted Domino server. Otherwise, the crawler will not be able to crawl anything. This critical step allows the Notes Client to configure your notes.ini so that the Notes API loads properly.
3. Create an IBM (Lotus) Notes user with the Reader Access

www.coveo.com
Before using the connector, an IBM Notes user must be configured with the Reader Access to all IBM Notes content that you wish to index.

4. Copy the user.id and the notes.ini files from the IBM Notes server to the Coveo Master server in the folder of your choice under the index configuration folder ([Index_Path]\Config) because these files are needed by the IBM Notes security provider and the connector.

   **Example:** D:\CES7\Config\Notes

5. Create a security mapping file (see "About the Notes Security Mapping File" on page 1036).

6. On the Coveo server, in the Coveo Administration Tool:

   a. Configure a user identity

   The Coveo connector needs an account to crawl your IBM Notes content. For this purpose, select an existing IBM Notes account or create a new one that has read access to all the content that you want to index.

   b. Create a security provider

   When you want to index IBM Notes security permissions, you must create a security provider (see "Configuring an IBM Notes Security Provider" on page 1043).

   c. Configure and index an IBM Notes source.

   The connector must know details about your IBM Notes instance to be able to index its content (see "Configuring and Indexing an IBM Notes Source" on page 1047).

   d. If you encounter issues, verify if modifying the default value of hidden source parameters can help resolve the problems (see "Modifying Hidden IBM Notes Source Parameters" on page 1053).

9.20.3 IBM Notes Connector Requirements

Your environment must meet the following requirements to be able to use the IBM Notes connector (formerly Lotus Notes connector):

- Coveo Enterprise Search 7.0

  The connector is available in all CES 7.0 versions.

- IBM Notes/Domino versions:

  - Supported version: 8.5.1 (8.5 is recommended)
  - Deprecated support versions: 7, 8

- Coveo license for the IBM Notes connector

  Your Coveo license must include support for the IBM Notes connector to be able to use this connector.

- IBM Notes Client (formerly Lotus Notes Client) installed on the Coveo Master server.
Notes:

- Ensure your Coveo Master server meets the IBM Notes Client requirements (see [Index of system requirements for Notes](#)).
- The version of IBM Notes Client must be the same version as IBM Notes/Domino.

- At least one database on the targeted server using the IBM Notes client.

**Note:** This mandatory step is to ensure the Notes settings file (notes.ini) is properly configured.

What's Next?

Create and configure an IBM Notes connector source (see "Configuring and Indexing an IBM Notes Source" on page 1047).

9.20.4 About the Notes Security Mapping File

The Notes security provider connects to the Domino address book database to retrieve metadata fields for all Notes users. With these fields, the security provider can form valid Windows usernames and then, using a security mapping file (XML file that contains a set of rules defining how the mapping process must be achieved), map Notes users to Windows users. There are two ways to map users: direct mappings and resolution methods.

You can refer to the following subsections for details on how to create a Notes security mapping file:

- When you only have a handful of Notes users or some user's account name that do not follow any specific pattern, use direct mappings (see "Creating a Notes Security Mapping File Using Direct Mappings" on page 1036).

- When you user's account name follow a specific pattern, use resolution methods along with the Notes Security Resolution tool to help you create and validate your Notes security mapping file (see "Creating and Validating a Notes Security Mapping File Using Notes Security Resolution Tool" on page 1038).

9.20.4.1 Creating a Notes Security Mapping File Using Direct Mappings

Direct mappings directly maps an IBM Notes user to its corresponding Windows user. Use it whenever a user’s account name does not follow any specific pattern. This also can be particularly useful when you only have a handful of users to map, or for diagnosis purposes.

**Important:** Whenever the security mapping file is modified, you have to restart the Notes security provider by clicking Apply Changes in the Modify Security Provider page of the Administration Tool. Otherwise, your security modifications will not be reflected in CES.

To create a Notes security mapping file using direct mappings

1. Open a text editor.

2. In the text editor, design direct mapping nodes (<DirectMapping></DirectMapping>) for each of your Notes users.
**Example:** Your security mapping file should look like the following:

```xml
<?xml version="1.0" encoding="utf-8" ?>
<SecurityMapping>
  <DirectMappings>
    <DirectMapping>
      <Lotus>John Smith</Lotus>
      <Windows>domain\user0124</Windows>
    </DirectMapping>
    <DirectMapping>
      <Lotus>CN=John Smith/O=domain @ domain</Lotus>
      <Windows>domain\user0124</Windows>
    </DirectMapping>
  </DirectMappings>
</SecurityMapping>
```

The first direct mapping node `<DirectMapping>` directly maps the IBM Notes user John Smith to the Windows user `domain\user0124`.

The second direct mapping node uses the complete LDAP syntax as the username in the Lotus node, i.e. `CN=John Smith/O=domain @ domain`. The domain part represents the name of the Domino domain the server is member of. The `@` character is mandatory.

**Note:** Remember that in the Domino address book on the server, each user has a field named **FullName**. This field is stored as an LDAP entry, such as `CN=John Smith/O=domain/OU=orgUnit`. You can enter either only the CN part as the username in the Lotus node `<Lotus>`), i.e. John Smith, or the complete LDAP syntax as in the second direct mapping node.

3. Using an administrator account, connect to the Coveo Master server.

4. Save the custom security mapping file on the Coveo Master server.

**Example:** `C:\ces7\Config\IBMSecurityMappingFile.xml`

5. Configure the connector to use the security mapping file in the IBM Notes security provider page (see "Security Mapping File Path" on page 1046).

**Notes:**

- Direct mappings have priority over resolution methods. In other words, any mapping entered as a direct mapping is used as is by the security provider, even if it is invalid (invalid Notes or Windows user).

- Direct mappings with a complete LDAP syntax have priority over direct mappings with a common name part only. In the example above, if there is a single John Smith in your organization, then use the short form (common name only). If there is more than one John Smith in your organization, then use the long form (full LDAP syntax). By using the short form, you take the risk of mapping the wrong Windows username to the wrong Notes username, as the short form queries the address book for the very first entry corresponding to John Smith.

- Users not specified as direct mappings are mapped using one of the resolution methods provided (if any). The first method is executed on the first user found in the Domino address book and if the Windows username being formed is invalid, the second method is executed and so on. If all resolution methods fail, no Windows user is mapped to the current IBM Notes user.
9.20.4.2 Creating and Validating a Notes Security Mapping File Using Notes Security Resolution Tool

Resolution methods are expressions that dictate how Windows usernames are formed from the Notes user's fields in the Domino address book. Use resolution methods whenever Notes user account names follow a specific pattern enabling a mapping pattern to be applied between users. The user account name pattern can be formed of string constants, fields from the Domino address book and regular expressions. Resolution methods can be particularly useful when you have a large address book.

**Note:** When you need more than one resolution method to map all your users, enable the Allow Multiple Resolution Methods parameter in the Notes security provider configuration page (see Configuring an IBM Notes Security Provider).

The NotesSecurityResolutionTool.exe command line tool that comes with CES can perform different operations to help you create and validate the security mapping file when using resolution methods.

**Important:** Whenever the security mapping file is modified, you have to restart the Notes security provider by clicking Apply Changes in the Modify Security Provider page of the Administration Tool. Otherwise, your security modifications will not be reflected in CES.
To create and validate a Notes security mapping file using the Notes security resolution tool

1. Understand how to design resolution methods.

Example: Resolution methods look like the following:

```xml
<?xml version="1.0" encoding="utf-8" ?>
<SecurityMapping>
  <ResolutionMethods>
    <ResolutionMethod MethodName="FirstAndLastNames">
      <Format>domain\{firstNameArg}\{lastNameArg}</Format>
      <Arguments>
        <Argument Name="firstNameArg">%[FirstName]</Argument>
        <Argument Name="lastNameArg">%[LastName]</Argument>
      </Arguments>
    </ResolutionMethod>
    <ResolutionMethod MethodName="FirstLetterLastName">
      <Format>domain\{firstLetterArg}\{lastNameArg}</Format>
      <Arguments>
        <Argument Name="firstLetterArg">RegEx=".*\b(\w)">%[FirstName]</Argument>
        <Argument Name="lastNameArg">%[LastName]</Argument>
      </Arguments>
    </ResolutionMethod>
    <ResolutionMethod MethodName="DomainFirstAndLastNames">
      <Format>\{domainArg\}\{firstLetterArg}\{lastNameArg}</Format>
      <Arguments>
        <Argument Name="domainArg">%[COVEO_ServerDomain]</Argument>
        <Argument Name="firstLetterArg">RegEx=".*\b(\w)">%[FirstName]</Argument>
        <Argument Name="lastNameArg">%[LastName]</Argument>
      </Arguments>
    </ResolutionMethod>
  </ResolutionMethods>
</SecurityMapping>
```

The first resolution method node (ResolutionMethod) combines the first name (%[FirstName]) and last name (%[LastName]) fields of IBM Notes users to form the corresponding Windows users. The syntax %[Field] identifies a specific field from the current Notes user in the Domino address book. For example, the current Notes user being mapped is John Smith. Its corresponding Windows user will be domain\JohnSmith.

The second resolution method node uses a regular expression to extract the first letter from the first name field of Notes users. It also uses the last name field, just like the first resolution method node does. If the first method fails while trying to map the user John Smith, the Windows user being mapped will be devdomain\JSmith.

The last method is almost identical to the second one, except that the domain name used to form Windows users is taken from the COVEO_ServerDomain field (%[COVEO_ServerDomain]). This is a special Coveo field with a value corresponding to the name of the current Domino server. If the second method fails and the current Domino server from which Notes users are extracted is named domino8.corp.domain.com; hence, the Windows user being mapped will be domino8.corp.domain.com\JSmith.

2. Open a text editor.

3. In a text editor, depending on your use case, write a basic file with a single resolution method.

www.coveo.com
Example: Your file content should look like the following:

```xml
<?xml version="1.0" encoding="utf-8"?>
<SecurityMapping>
  <ResolutionMethods>
    <ResolutionMethod MethodName="FirstLetterLastName">
      <Format>domain\{firstLetterArg}\{lastNameArg}</Format>
      <Arguments>
        <Argument Name="firstLetterArg" RegEx=".*\b([^\w]*)">%
        </Argument>
        <Argument Name="lastNameArg">%
      </Arguments>
    </ResolutionMethod>
  </ResolutionMethods>
</SecurityMapping>
```

4. Save the file with an XML extension (.xml) and remember the file path.

5. Open Command Prompt.

6. In Command Prompt, reach the folder where CES.NotesSecurityResolutionTool.exe is installed.

   **Note:** The tool is located in the Coveo Enterprise Search 7\Bin\Win32 folder, for instance: C:\Program Files\Coveo Enterprise Search 7\Bin\Win32.

7. Optionally, list all available fields for a Notes user by adapting the following command line to match your needs (see "Notes Security Resolution Tool References" on page 1042):

   ```
   ```

   For the /p:<string> parameter, enter the complete path to the file created in step 3.

   If your command line is valid, the tool will ask you to enter the password for the ID file you used.

   **Note:** The output contains all available fields and their values. If needed, use this as a reference to design new resolution methods.

8. Optionally, generate a complete report about the resolution method(s) in the basic file created in step 3 by adapting the following command line to match your needs (see "Notes Security Resolution Tool References" on page 1042):

   ```
   ```

   For the /p:<string> parameter, enter the complete path to the file created in step 3 or updated in step 7.

   If your command line is valid, the tool will ask you to enter the password for the ID file you used.

   **Note:** For each resolution method, the report file (output file generated by the /o:<string> parameter) lists all Windows users that were either successfully or unsuccessfully mapped from Notes users. Ensure that all the users that you want to map are validated in the report. If not, review your resolution method(s), before proceeding to step 9.

9. Generate a complete security mapping file starting with a single resolution method:
a. In a text editor, design a new resolution method with the information obtained in step 7 and step 8, or open the basic file created in step 3.

b. Under the closing ResolutionMethods node, add an empty DirectMappings node (<DirectMappings></DirectMappings>).

c. Save the file.

d. In Command Prompt, use the following command line adapted to your needs (see “Notes Security Resolution Tool References” on page 1042):

```bash
```

For the /p:<string> parameter, enter the complete path to the file created in step 3 or the modified file in step 7 or step 8 depending on your case.

If your command line is valid, the tool will ask you to enter the password for the ID file you used.

**Note:** For each successful user mapping (a corresponding Windows user was found for the Notes user being currently processed), a DirectMapping node is created and appended to the output XML file (generated by the /o:<string> parameter). By using DirectMapping nodes rather than ResolutionMethod nodes, validation is not required by the security provider and therefore processing them is much faster.

e. In a text editor:

i. Open the output XML file.

ii. Copy all the direct mapping nodes (<DirectMapping></DirectMapping>) generated by the tool.

iii. Create a new file and paste the direct mapping nodes between security mappings nodes (<DirectMappings></DirectMappings>) in another XML file.

**Example:** Your security mapping file should look like the following:

```xml
<?xml version="1.0" encoding="utf-8" ?>
<SecurityMapping>
  <DirectMappings>
    <DirectMapping>
      <Lotus>John Smith</Lotus>
      <Windows>domain\jsmith</Windows>
    </DirectMapping>
    <DirectMapping>
      <Lotus>Jack Johnson</Lotus>
      <Windows>domain\jjohnson</Windows>
    </DirectMapping>
  </DirectMappings>
</SecurityMapping>
```

iv. Save the file in the Coveo Enterprise Search 7\Config folder, for instance C:\Program Files\Coveo Enterprise Search 7\Config.

v. Enter the path to this file in the Security Mapping File Path box in the Notes security provider creation page (see “Security Mapping File Path” on page 1046).
### 9.20.4.2.1 Notes Security Resolution Tool References

The following are the available parameters in the tool:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Long form</th>
<th>Required</th>
<th>Short form</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Server Name</td>
<td>/ServerName:&lt;string&gt;</td>
<td>✓</td>
<td>/s:&lt;string&gt;</td>
<td>Domino server that contains the Global address book database.</td>
</tr>
<tr>
<td>User ID File Path</td>
<td>/UserIdFilePath:&lt;string&gt;</td>
<td>✓</td>
<td>/id:&lt;string&gt;</td>
<td>Complete path of the user.id file. If not specified, the default data path of the current IBM Notes installation is used.</td>
</tr>
<tr>
<td>Security Mapping File</td>
<td>/SecurityMappingFilePath:&lt;string&gt;</td>
<td>✓</td>
<td>/p:&lt;string&gt;</td>
<td>Complete path to the basic file containing your resolution method(s).</td>
</tr>
<tr>
<td>Output File Path</td>
<td>/OutputPath:&lt;string&gt;</td>
<td>✓</td>
<td>/o:&lt;string&gt;</td>
<td>Complete path to the output file. Format can be either text or XML, depending on the XmlOutput parameter.</td>
</tr>
<tr>
<td>Temporary Path</td>
<td>/TempPath:&lt;string&gt;</td>
<td>✓</td>
<td>/t:&lt;string&gt;</td>
<td>Folder used by the tool to store its temporary files.</td>
</tr>
<tr>
<td>IBM Notes Data Path</td>
<td>/NotesDataPath:&lt;string&gt;</td>
<td></td>
<td>/d:&lt;string&gt;</td>
<td>Complete path to the Data folder of the current IBM Notes installation.</td>
</tr>
<tr>
<td>IBM Notes Settings File Path</td>
<td>/NotesINIFilePath:&lt;string&gt;</td>
<td></td>
<td>/ini:&lt;string&gt;</td>
<td>Complete path to the Notes Settings file (notes.ini). To be used with a multi-user Notes install.</td>
</tr>
<tr>
<td>Show fields for user</td>
<td>/ShowFieldsForUser[+</td>
<td>-]</td>
<td></td>
<td>/show[+</td>
</tr>
<tr>
<td>Xml Output</td>
<td>/XmlOutput[+</td>
<td>-]</td>
<td></td>
<td>/xml[+</td>
</tr>
<tr>
<td>Parameter</td>
<td>Long form</td>
<td>Required</td>
<td>Short form</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------------</td>
<td>----------------------------</td>
<td>----------</td>
<td>------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Include Valid Securities</td>
<td>/IncludeValidSecurities[+</td>
<td>-]</td>
<td></td>
<td>/vm[+</td>
</tr>
</tbody>
</table>

| Include Invalid Securities| /IncludeInvalidSecurities[+|-] |          | /im[+|-]  | Output or not (im-) the invalid user mappings found using the resolution methods as new DirectMapping nodes inside the XML output file (Xml Output parameter must be activated). Default value is im-. |

9.20.5 Configuring an IBM Notes Security Provider

The Coveo IBM Notes connector fully supports the IBM Notes security model. When you want users searching for IBM Notes content in a Coveo search interface to only see the content to which they have access in IBM Notes, the connector needs a security provider to be able to index the permissions for each indexed IBM Notes item.

**Note:** You can get familiar with how Coveo components deal with permissions on documents both at indexing and query time.

To configure an IBM Notes security provider

1. On the Coveo server, access the Administration Tool.
3. In the navigation panel on the left, click Security Providers.
4. In the Security Providers page, click Add to create a new security provider.
5. In the Modify Security Provider page:
a. Configure the following required parameters:

Name

Choose a meaningful name to identify the security provider.

Example: Notes
Security Provider Type

In the drop-down list, select Notes (x86).

User Identity

In the drop-down list, select the user identity that you selected or created previously (see IBM Notes Connector Deployment Overview).

Active Directory Security Provider

In the drop-down list, select Active Directory or the active directory security provider type that you created to allow this security provider to resolve and expand the groups (see IBM Notes Connector Deployment Overview).

Domino Server Name

Enter the name of the Domino server that holds the IBM (Lotus) Notes address book (Domino Directory\names.nsf). You must leave the Domino Server Name box empty when the Personal address book is used. One of the possible name form is the Notes hierarchical format \[Department]/\[Company name].

Note: The Domino server name is located above the Inbox folder to the left of your Mail Inbox view.

Examples:

- Sales/IBM (Notes hierarchical format)
- domino8 [IBM (Lotus) Notes Server Version]
- maple.ibm.com (Website)
- 172.16.254.1 (IP address)

User ID File Path

Enter the full path to the user.id file that you copied from the IBM Notes server to be used to be used by the connector to authenticate to the Domino server (see IBM Notes Connector Deployment Overview). If left empty, this parameter is assigned the complete path of the current or last user.id used in the IBM Notes client.

Example: C:\CES7\Config\user.id
Security Mapping File Path

Enter the full path to the security mapping file you created (see IBM Notes Connector Deployment Overview).

Example: C:\CES7\Config\NotesSecurityMappingFile.xml

Notes:

- The mapping of IBM Notes users to their corresponding Windows users is achieved by the security provider using this file.
- When you are unable to create a security mapping file, contact Coveo Support for assistance.

Temporary Working Folder Path

Enter the full path to the folder on the Coveo server where temporary files are stored by the security provider. This folder must be unique for each security provider.

Example: C:\tmp\NotesSecurityProvider

Notes Setting File (.ini) Path

Enter the full path to the notes.ini file that you copied from the IBM Notes server to be used by the connector to initialize the Notes API (see IBM Notes Connector Deployment Overview). This file contains configuration information and user preferences. This is the notes.ini created by the IBM Notes Client installation (local notes.ini). If left empty, this parameter is assigned the path of the current IBM Notes installation.

Example: C:\CES7\Config\notes.ini

b. Review the value for the following optional default parameters that often do not need to be modified:

Allow Multiple Resolution Methods

Whether the security mapping file contains multiple resolution methods. When enabled, this parameter make sure every Windows username being formed is validated against the Active Directory.

Enable Safe Mode

Whether the crawling safe-mode is enabled, to avoid conflicts when crawling corrupted Notes databases.

Important: When this parameter is used, you must also add the parameter to the corresponding security provider. Otherwise, the crawling in safe-mode is going to be in a deadlock state when two competing actions are each waiting for the other to finish, and thus neither ever does. Furthermore, crawling in safe-mode is significantly slower comparing to the normal crawling process.

Safe Mode Timeout Time

When the Enable Safe Mode option is selected, this parameter is used to define the timeout time (in milliseconds) on the global mutex that protects the Notes API by blocking the connection to one at a
time. The default value is 60000 ms.

**Important:** Do not change the value of this parameter unless instructed by Coveo Support.

### Address Book Expansion Timeout Time

The timeout value (in milliseconds) allowed for the initial expansion of the Domino address book. The default value is 30000 ms.

**Note:** This process normally takes less than 30 seconds, but with very large address books, the expansion can take as long as several minutes. Adjust this value according to your needs. Once the entire list is built, the connector goes through all users to retrieve the required fields.

### Users Cache Life Time

The refresh interval (in minutes) of the users cache (local copy of the Domino address book). The default value is 1440 min (24 h).

**Example:** When you are performing permission tests, you can temporary reduce this value to a short period such as five minutes to ensure that your permissions changes and notes are quickly made available to the connector. Do not forget to return the parameter to its default value when you are done to prevent overloading the notes server.

**Note:** When your Domino address book is modified frequently (users are added or deleted), decrease the **Users Cache Life Time** parameter value here and in your Notes sources with the **UsersCacheLifeSpan** hidden parameter, so the users cache is updated regularly with the latest user additions/deletions in the Domino address book by synchronization (see "Modifying Hidden IBM Notes Source Parameters" on page 1053).

### Global Query Timeout Time

The timeout value (in milliseconds) allowed for a query to be executed against the Global address book database before sending an error message. The default value is 30000 ms.

**Note:** This process normally takes less than 30 seconds, but with very large systems, the process can take as long as several minutes. Adjust this value according to your needs.

c. Click **Add Parameter** when you want to show and change the value of advanced source parameters (see "Modifying Hidden IBM Notes Source Parameters" on page 1053).

d. Leave the **Allow Complex identities** cleared as it does not apply to this type of security provider.

e. Click **Apply Changes**.

### What's Next?

Create and index a source (see "Configuring and Indexing an IBM Notes Source" on page 1047).

### 9.20.6 Configuring and Indexing an IBM Notes Source

A source defines a set of configuration parameters for a specific IBM Notes database (contained in a NSF file). When you want to index more than one IBM Notes database, configure one source with all the database paths.
To configure and index a source with the IBM Notes connector

1. On the Coveo server, access the Administration Tool.
2. Select **Index > Sources and Collections**.
3. In the **Collections** section:
   a. Select an existing collection in which you want to add the new source.
   OR
   b. Click **Add** to create a new collection.
4. In the **Sources** section, click **Add**.
5. In the **General Settings** section of the **Add Source** page:

   a. Enter the appropriate value for the following required parameters:

   **Name**
   
   Enter a descriptive name of your choice for the connector source.

   **Example:** IBM Notes
Source Type

The connector used by this source. In this case, select **Notes**.

Addresses

Enter the list of starting addresses directly linking to the Notes Storage Facility files (.nsf) or the folder that contains the databases for the connector. When you want to have different security parameters for every database, you need to create a source for each database.

**Note:** For releases after IBM (Lotus) Notes 8, open the **Open Application** dialog (**File > Open > IBM (Lotus) Notes Application** or **CTRL + o**) and retrieve the Domino server name from the **Look in** field and the database path in the **File name** field.

**Example:**

![Open Application dialog](image)

**Examples:** The database file path can be:

- `notes://dominoserver/path/`
- `notes://dominoserver.company.com/mail/tuser1.nsf`
- `notes://111.111.111.111/path/database.nsf`
- `notes:///path/database.nsf/>ViewName`

**Note:** The scheme `notes:///` is used to index local Notes databases.

**Fields**

In the drop-down list, select the **Default Scheme** to use the default fields. If you are using a custom
mapping file, create a corresponding custom field set and select it.

b. Review the default value for the following parameters that often do not need to be modified:

**Rating**

Change this value only when you want to globally change the rating associated with all items in this source relative to the rating to other sources.

**Example:** If this source was for former employees email database, you may want to set this parameter to *Low*, so that in the search interface, results from this source appear later in the list compared to those from other sources.

**Document Types**

If you defined custom document type sets, ensure to select the most appropriate for this source.

**Active Languages**

If you defined custom language sets, ensure to select the most appropriate for this source.

**Refresh Schedule**

Select the time interval at which a full refresh of the source is automatically performed to keep the index content up-to-date. The default and recommended value is *Every day* especially when you add and remove users regularly.

6. In the **Specific Connector Parameters & Options** section of the **Add Source** page:

<table>
<thead>
<tr>
<th>Specific Connector Parameters &amp; Options</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>User ID File Path</strong></td>
</tr>
<tr>
<td>C(\text{C5%_Config})\text{userid}</td>
</tr>
<tr>
<td><strong>Notes Settings File Path</strong></td>
</tr>
<tr>
<td>C(\text{C5%_Config})\text{notes.ini}</td>
</tr>
<tr>
<td><strong>Number of Refresh Threads</strong></td>
</tr>
<tr>
<td>1</td>
</tr>
<tr>
<td><strong>Max Number of Retries</strong></td>
</tr>
<tr>
<td>3</td>
</tr>
<tr>
<td><strong>Server Query Timeout</strong></td>
</tr>
<tr>
<td>30</td>
</tr>
<tr>
<td><strong>Ignored Forms</strong></td>
</tr>
<tr>
<td>PreIdentificationServerParameterOrganiz</td>
</tr>
<tr>
<td><strong>Parameters</strong></td>
</tr>
<tr>
<td>Add Parameter</td>
</tr>
</tbody>
</table>

a. Review the following parameters that need to be filled:

**User ID File Path**

Enter the full path to the same user.id file than the one specified in the security provider configuration (see "Configuring an IBM Notes Security Provider" on page 1043). If left empty, this parameter is assigned the
complete path of the current or last user.id used in the IBM Notes client. The same value than the one entered in the security provider.

**Example:** C:\CES7\Config\user.id

**Note Settings File Path**

Enter the full path to the same notes.ini file than the one specified in the security provider configuration (see "Configuring an IBM Notes Security Provider" on page 1043). If left empty, this parameter is assigned the path of the current IBM Notes installation.

**Example:** C:\CES7\Config\notes.ini

b. Review if you need to change the default values for the following parameters:

**Number of Refresh Threads**

Determines the number of threads used while crawling IBM Notes items. The default and recommended value is 1.

**Note:** When you use more threads, you increase the possibilities that the crawling process stops in a case of a database with corrupted documents.

**Max Number of Retries**

Number of retries done for each call to the Notes API. The default and recommended value is 3.

**Note:** After the retries, the current query is suspended often causing the crawling process to stop. In any case, this is handled as a timeout by the connector.

**Server Query Timeout**

The maximum time (in seconds) allowed for a call to the Notes API to execute and complete. The default and recommended value is 30 sec.

**Ignored Form**

The list of IBM Notes forms (formerly Lotus Notes Forms) ignored while crawling and indexing documents. By default, this parameter is assigned an exhaustive list of common forms that should not be indexed by the connector. You can update this parameter by appending semicolon separated values, where the value is the name of a form.

Usually, this parameter is used to ignore system forms used internally by Notes and do not contain any relevant information for indexing purposes.

**Note:** Any other form type in the database should have the corresponding field mappings defined.

c. In the **Parameters** section, click **Add Parameter** to be able to change the default value of hidden parameters (see "Modifying Hidden IBM Notes Source Parameters" on page 1053).

d. In the **Option** section, review the default value of the following check boxes:
Index the document’s metadata

When selected, CES indexes all the document metadata, even metadata that are not associated with a field. The orphan metadata are added to the body of the document so that they can be searched using free text queries.

When cleared (default), only the values of system and custom fields that have the Free Text Queries attribute selected will be searchable without using a field query.

Example: A document has two metadata:

- `LastEditedBy` containing the value Hector Smith
- `Department` containing the value RH

In CES, the custom field `CorpDepartment` is bound to the metadata `Department` and its Free Text Queries attribute is selected.

When the Index the document’s metadata option is cleared, searching for RH returns the document because a field is indexing this value. Searching for hector does not return the document because no field is indexing this value.

When the Index the document’s metadata option is selected, searching for hector also returns the document because CES indexed orphan metadata.

Generate a cached HTML version of indexed documents

When you select this check box (recommended), at indexing time, CES creates HTML versions of indexed documents. In the search interfaces, users can then more rapidly review the content by clicking the Quick View link rather than opening the original document with the original application. Consider clearing this check box only if you do not want to use Quick View links or to save resources when building the source.

Open results with cached version

Leave this check box cleared (recommended) so that in the search interfaces, the main search result link opens the original document with the original application. Consider selecting this check box only when you do not want users to be able to open the original document but only see the HTML version of the document as a Quick View. In this case, you must also select Generate a cached HTML version of indexed documents.

7. In the Security section of the Add Source page:
a. In the **Security Provider** drop-down list, when you chose to use a security provider, select the security provider that you created for this source (see "Configuring an IBM Notes Security Provider" on page 1043).

b. In the **Authentication** drop-down list, select the user identity that you created for this source.

c. Click **Save** to save the source configuration.

8. On the toolbar, click **Start/Rebuild** to start indexing your source.

9. Validate that the source building process is executed without errors:

   - In the navigation panel on the left, click **Status**, and then validate that the indexing proceeds without errors.

   OR

   - Open the CES Console to monitor the source building activities.

**What's Next?**

Set an incremental refresh schedule for your source to maintain your source up-to-date with the IBM Notes database between full refreshes.

9.20.7 Modifying Hidden IBM Notes Source Parameters

The **Add Source** and **Source: ... General** pages of the Administration Tool present the parameters with which you can configure the connector for most IBM Notes setups. More advanced and more rarely used parameters are hidden. You can choose to make one or more of these parameters appear in the **Add Source** and **Source: ... General** pages of the Administration Tool so that you can change their default value. Consider changing values of hidden parameters when you encounter issues.

The following list describes the advanced hidden parameters available with IBM Notes sources. The parameter type (integer, string…) appears between parentheses following the parameter name.

**TreatLookupErrorsAsWarnings (Boolean)**

This is used to ignore any error during user lookup in the Domino address book at the beginning of an indexing run. The default value is false.

**HandledNetworkErrorCodes (String)**

This parameter is used to define the list of network error codes handled by the connector as fatal exceptions,
that is, error codes that will stop any indexing run (without wiping out the entire index). The default values are
2055, 2561, 2562, 2570, 2604, 2645, 7267, 7287.

**UsersCacheLifeSpan (Integer)**

This parameter is used to define the life span of the users cache built from the Domino address book. Once the
default 24-hour period has passed, the next crawling run (Rebuild/Refresh/Live Indexing) will trigger an update
of the users cache. This update is not a complete rebuild; the connector only considers modifications made to
the Domino address book since the last rebuild/update of the users cache. The default value is 1440 min (24 h).

**AddressBookServerURL (String)**

This parameter is used to customize the address book server used by the connector. The address book is used
to retrieve several fields from Notes users, such as their email address, mail filenames, etc. The correct syntax
for this parameter is either: notes://[server_name] for a specific Domino server or notes:/// for a local
server (personal address book). The default value is none.

**LocalDatabaseMappingFilePath (String)**

This parameter is used to specify a mapping file specifically for local Notes databases. The mapping file can be
used to override security permissions and to fill emailsearch-related fields on indexed documents, even if your
Personal address book is incomplete. With a mapping file that is properly configured, you can crawl both remote
and local databases using the same source, meaning that you can have a security provider assigned to your
source (for remote databases) and also a mapping file (for local databases). When you don't use this parameter,
the current security permission option in your source will be used for local databases. Basically, it means that
e-mailsearch-related fields as well as security permissions may be incorrect on indexed documents. The default
value is none.

**GetFormsTimeout (Integer)**

This is the time period (in seconds) allowed for the extraction of forms and fields when we access the Fields
section of a Notes source. The extraction can take up to several minutes, depending on the complexity of your
database design. The default value is 30 sec.

**DisableSecurityMappingCache (Boolean)**

Select **true** would disable the SecurityMappingCache. When every single document has a different security,
changing the value to **true** could speed up the crawling. For most other setups, changing the
DisableSecurityMappingCache value for **true** significantly slows down the crawling process. The default
value is **false**.

**IgnoreDatabaseSecurityChangeOnLiveIndexing (Boolean)**

The default value is **false**. True would disregard any security change on a database when live indexing. It still
would update those changes to the internal structures, but would not reindex because of them. Unless you
know that the security has not changed, it is not recommended to use this flag as it will go over security
changes.

**SampleDatabase (Boolean)**

The default value is **true**. Change the value to **false** when you want to edit the field mappings.

Use the following procedure only when you want to modify one or more of the above hidden source parameters.
To modify hidden IBM Notes source parameters

1. Refer to "Adding an Explicit Connector Parameter" on page 450 to add one or more IBM Notes hidden source parameters.

2. For a new IBM Notes source, access the Add Source page of the Administration Tool to modify the value of the newly added advanced parameter:
   a. Select Index > Sources and Collections.
   b. Under Collections, select the collection in which you want to add the source.
   c. Under Sources, click Add.
   d. In the Add Source page, edit the newly added advanced parameter value.

3. For an existing IBM Notes source, access the Source: ... General page of the Administration Tool to modify the value of the newly added advanced parameter:
   a. Select Index > Sources and Collections.
   b. Under Collections, select the collection containing the source you want to modify.
   c. Under Sources, click the existing IBM Notes source in which you want to modify the newly added advanced parameter.
   d. In the Source: ... General page, edit the newly added advanced parameter value.

4. Rebuild your IBM Notes source to apply the changes to the parameters.

9.20.8 Troubleshooting IBM Notes Connector Issues

NameLookups are limited on this server to a size smaller than what would be returned. See your Domino Administrator for more information.

Possible cause

The global address book on the server contains too many entries to be returned in a single batch. The server is not configured to handle this.

Possible solution

Add the NAMELOOKUP_MAX_MB variable in notes.ini on the server. Assign it a value of 2 (MB), then increase it gradually until you no longer see the error message. Otherwise, it is possible to add the custom source parameter TreatLookupErrorsAsWarnings and set it to True (see Modifying Hidden IBM Notes Source Parameters). However, expect the metadata fields to have incorrect email addresses.

Unable to instantiate the Lotus Notes classes: Failed to read from an IPC port: The pipe has been ended.

Possible causes

- The timeout value is not large enough when initializing the Notes API.
- The notes.ini file being used by the connector is invalid.
More than one Notes source is running and one of them is currently crawling a corrupted database. Thus, one of the sources stopped.

Possible solutions

- Increase the value of the source parameter **Server Query Timeout**.
- Configure the `notes.ini` file properly by opening at least one database on the targeted Domino server using the Notes client installed on the CES server.
- Add the parameter **EnableSafeMode** on all Notes sources and on the Notes security provider (see "Modifying Hidden IBM Notes Source Parameters" on page 1053 and "Configuring an IBM Notes Security Provider" on page 1043).

Mapping (FormType) not found in the metadata mappings.

Possible cause

There is no mapping defined for the specified form type.

Possible solution

Define the mapping for the specified form type through the **Fields** section of your source. Otherwise, ignore this form by adding it to the **Ignored Forms** source parameter (see "Modifying Hidden IBM Notes Source Parameters" on page 1053).

Closing the Notes processes and resetting the API. Additionally, if CES is running in standalone mode (CSService7.exe –standalone), you may see empty command prompt windows popping up intermittently.

Possible cause

The connector tried to retrieve a corrupted document but the Notes API crashed by doing so.

Possible solution

There is no required user action; the connector handles this situation automatically by resetting the API to a proper state and resuming the crawling where it stopped.

Note: Any other process using the Notes API will be aborted (Lotus Notes client, Domino Administrator, Domino Designer, ...). If other Notes sources may run at the same time, refer to the Configuration section of this documentation, specifically for the **EnableSafeMode** parameter (see "Modifying Hidden IBM Notes Source Parameters" on page 1053).

Cannot load security provider: [error/warning message]

Possible cause

An invalid parameter prevents the security provider from loading.

Possible solution

Read the error message carefully as it describes the cause of the error. In case no error/warning message is displayed, either the **DLL Path** or the **AssemblyPath** parameter is incorrect (see "Configuring an IBM Notes
Only one Resolution Method is allowed for the Notes Security Provider. To use several resolution methods, use the AllowMultipleResolutionMethods parameter.

Possible cause

The security mapping file contains either no resolution method or several resolution methods although the Allow Multiple Resolutions Methods parameter was not enabled (see "Configuring an IBM Notes Security Provider" on page 1043).

Possible solutions

- Define at least one resolution method in the security mapping file if it does not contain any.
- In case several resolution methods are used, select the Allow Multiple Resolutions Methods checkbox in the security provider parameters list (see "Configuring an IBM Notes Security Provider" on page 1043).

class Notes::DatabaseOpenFailedException: Unable to find path to server. Check that your network connection is working. If you have a working connection, go to Preferences - Notes Ports and click Trace to discover where it breaks down. (2051)

Possible cause

Either the notes.ini file or the user.id file used by the connector or the security provider is invalid for the targeted Domino server.

Possible solution

Make sure that the notes.ini file is properly configured to connect to the targeted Domino Server. Otherwise, verify that the user.id file has proper access to the Domino server.

Getting a blank page when accessing the Fields section of a Notes source.

Possible symptoms

- As soon as you try to access the section, you get a blank page.
- You try to access the section but it takes a while before you get the blank page (about 1min 30sec)

Possible causes

- The credentials you use in your source are incorrect (user identity), or there is some network problem (server unreachable).
- Retrieving the fields and forms from the database(s) in the starting address(es) takes too much time, either because the design complexity of these database(s) is high or because the network connection is slow.

Possible solutions

- Fix the user identity used by your source. The password is most likely incorrect. Also, make sure that you can ping the servers pointed to by your starting addresses.
- Add the GetFormsTimeout parameter to your source. The default value is 30 sec. Increase its value until you no longer get the blank page (see Modifying Hidden IBM Notes Source Parameters).

The source parameter "SampleDatabase" doesn't exist. The modifications were not saved.

Possible cause
- You try to edit the field mappings.

Possible solutions
- Add the SampleDatabase parameter to your source. The default value is true. Change that value to false when you want to edit the field mappings (see Modifying Hidden IBM Notes Source Parameters).

9.21 Jive Connector

**CES 7.0.5388+ (April 2013)**

The Coveo connector for Jive 9 allows you to index and integrate the content of your Jive spaces and groups into your Coveo unified index, making it easily searchable by end-users.

**Notes:**
- Deprecated support versions: Jive 6, 7, and 8
- **CES 7.0.8996+ (June 2017)** Support for Jive 9.
- **CES 7.0.8047+ (December 2015)** Support for Jive 8.
- You can also index content from Jive 5, Jive SBS, or Clearspace using the Jive 5/SBS/Clearspace connector.

9.21.1 Connector Features Summary

<table>
<thead>
<tr>
<th>Features</th>
<th>Supported</th>
<th>Additional information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Jive version</td>
<td>9 and Cloud</td>
<td>(For Jive Cloud only) Following available Jive Cloud releases</td>
</tr>
</tbody>
</table>
| Searchable content types | ✔️                 |  - Communities (also known as Spaces), social groups (also known as groups), projects, people and their profile, direct messages (requires Coveo plugin), documents (private and public), discussions (private and public), blog posts (for spaces, projects, users, groups and system blogs), announcements, polls, comments (for documents, blog posts, and polls), attachments (for documents, blog posts, and discussions), ideas (private and public), and videos (private and public).  
  - Support phrase substitutions (requires Coveo plugin), tags, and categories. |
### Features

<table>
<thead>
<tr>
<th>Features</th>
<th>Supported</th>
<th>Additional information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Content update</td>
<td></td>
<td>(Jive 8 and 9 only) Full refresh or rebuild needed to retrieve (due to Jive REST API limitations):</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Comments on comments and replies on replies</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Deleted file items.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>The Coveo plugin is required to:</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Note:</strong> The plugin cannot be installed in Jive Cloud.</td>
</tr>
<tr>
<td>Incremental refresh</td>
<td>✔</td>
<td></td>
</tr>
<tr>
<td>Full refresh</td>
<td>✔</td>
<td></td>
</tr>
<tr>
<td>Rebuild</td>
<td>✔</td>
<td></td>
</tr>
<tr>
<td>Document-level security</td>
<td>✔</td>
<td>- Requires the Coveo plugin for Jive on-premises instances.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Not supported for Jive Cloud. Permissions must be manually defined on the source.</td>
</tr>
</tbody>
</table>

#### 9.21.2 Features

- Content Indexing
  - Retrieval and indexing of the following Jive object types:
    - Spaces (also known as Communities)
    - Groups
    - Projects (with related Tasks and Checkpoints)
    - People and their profiles
    - Direct messages
    - Documents (private and public)
    - Discussions (private and public)
    - Blog posts (for spaces, projects, users, groups and system blogs)
    - Announcements
    - Polls
    - Comments (for documents, blog posts, and polls)
    - Attachments (for documents, blog posts, and discussions)
Ideas (private and public)

Videos (private and public)
  - Support for phrase substitution
  - Support for tags and categories

Security

The connector indexes the permissions on Jive objects. Consequently, Coveo search results only contain Jive objects that the end-user can access within the Jive communities. Permission indexing is done using an optional plugin.

**Note:** You cannot install the Coveo plugin in Jive Cloud.

Incremental refresh

The connector periodically queries Jive for the latest edits, keeping the index content up-to-date.

**Notes:**

- **CES 7.0.8691+ (December 2016)** The incremental refresh takes account of deleted events (requires the Coveo plugin) (see "Installing the Coveo Plugin on Your Jive Server" on page 1066).
- **CES 7.0.8541– (September 2016)** A source full refresh or rebuild is required to remove deleted events from the index.
- For Jive 8 **CES 7.0.8047+ (December 2015)** and 9 **CES 7.0.8996+ (June 2017)** spaces, due to a Jive REST API limitation, only the first level of comments on documents and replies on discussions are indexed by an incremental refresh, meaning that comments on comments and replies on replies cannot currently be retrieved unless performing a full refresh or source rebuild.
- Since the Jive REST API does not provide the list of deleted File items, a source full refresh or rebuild is required to take the deletion of File items into account.

Feature history

<table>
<thead>
<tr>
<th>CES version</th>
<th>Monthly release</th>
<th>Features</th>
</tr>
</thead>
<tbody>
<tr>
<td>7.0.8996</td>
<td>June 2017</td>
<td>Support for Jive 9</td>
</tr>
<tr>
<td>7.0.8691</td>
<td>December 2016</td>
<td>Incremental refresh for events</td>
</tr>
<tr>
<td>7.0.8047</td>
<td>December 2015</td>
<td>Support for Jive 8</td>
</tr>
<tr>
<td>7.0.7599</td>
<td>April 2015</td>
<td>Support for Jive 7</td>
</tr>
<tr>
<td>7.0.6607</td>
<td>April 2014</td>
<td>Support for Jive Cloud (version 8)</td>
</tr>
<tr>
<td>7.0.5785</td>
<td>August 2013</td>
<td>Updated plugin to resolve incremental refresh issues</td>
</tr>
<tr>
<td>7.0.5388</td>
<td>April 2013</td>
<td>Connector introduction</td>
</tr>
</tbody>
</table>
What’s Next?

Get familiar with the deployment steps (see “Jive Connector Deployment Overview” on page 1061).

9.21.3 Jive Connector Deployment Overview

The following procedure outlines the steps needed to deploy the Jive connector. The steps indicate the order in which you must perform configuration tasks on both the Jive and Coveo servers.

To deploy the Jive connector

1. Validate that your environment meets the requirements (see “Jive Connector Requirements” on page 1062).

2. On the Jive server:
   a. Choose a Jive crawling account

   You must choose which Jive account the Coveo connector uses to crawl the content of your Jive communities (see "Creating a Jive Crawling Account" on page 1063).

   b. Optionally install the Coveo for Jive plugin

   Install the Coveo plugin used by the connector on your Jive server. The plugin is optional but enables several connector features such as allowing to index permissions (see "Installing the Coveo Plugin on Your Jive Server" on page 1066).

   **Note:** Because you cannot install the Coveo for Jive plugin in Jive cloud, Coveo cannot index permissions for this content.

   **Tip:** In rare cases where the Jive 6+ browse index is not synchronized with the master data, the Jive API may not return all documents to the Coveo connector. To prevent missing some Jive documents in your Coveo index, ensure that your Jive indexes are up to date (from the Jive Admin Console **System > Settings > Browse > Re-synchronize browse index**).

3. On the Coveo server:
   a. Create a user identity

   You must create a user identity to hold the credentials of the Jive crawling account that you selected.

   b. **CES 7.0.7711+ (June 2015)** Optionally create an email security provider

   When the primary email is defined for each of your users in Jive and this email is used to authenticate them in your Coveo search interface, you can create an Email security provider to allow you to map your Jive users to their email (see "Configuring an Email Security Provider" on page 65).

   c. Optionally create a Jive security provider

   When you installed the Coveo plugin and want to index Jive permissions, you must create a security provider that the connector uses to resolve indexed permissions into a list of Jive users and groups (see "Configuring a Jive Security Provider" on page 1068).

   d. **CES 7.0.8541+ (September 2016)** Create a Jive field set
It is recommended to import the out-of-the-box Jive field set `{[CES_Path]\Bin\Coveo.CES.CustomCrawlers.Jive.FieldSet.xml to be able to easily add Confluence-specific facets to your Coveo search interfaces.

e. Create and index a source

You must create a source describing the Jive community to index (see "Configuring and Indexing a Jive Source" on page 1072).

4. Troubleshooting

a. Review known issues (see "Troubleshooting Jive Connector Issues" on page 1081).

b. Consider modifying some hidden source parameters to try resolving other issues (see "Modifying Hidden Jive Source Parameters" on page 1081).

5. Allow Jive users to be authenticated in a Coveo search interface

When your Jive community is not integrated with Active Directory, your end-users need to sign in to Jive in a Coveo search interface to be able to see Jive content in search results. In this case, you need to add the Jive security provider to your search interface to allow end-user to sign in to Jive (see "Adding Security Providers to a .NET Search Interface" on page 631).

9.21.4 Jive Connector Requirements

Your environment must meet the following requirements to be able to use the Jive connector:

- Coveo license for the Jive connector

Your Coveo license must include support for the Jive connector to be able to use this connector. You can see the currently supported connectors from the Administration Tool.

- CES 7.0.5388+ (April 2013)

- Jive product versions

  - Supported versions:

    - Jive Cloud (2015.2.2)

      The connector supports the cloud version of Jive, however because the optional Coveo plugin cannot be installed in this version of Jive, the plugin features such as indexing permissions are not available (see "Plugin Benefits" on page 1066).

    - Jive 9 CES 7.0.8996+ (June 2017)

      Note: The optional Coveo plugin can be installed on Jive-hosted and self-hosted instances.

  - Deprecated support versions: 6, 7, and 8
What's Next?

Choose which Jive account the Coveo connector uses to crawl the content of your Jive communities (see "Creating a Jive Crawling Account" on page 1063).

9.21.5 Creating a Jive Crawling Account

The Coveo connector needs a Jive account to be able to crawl the content of your Jive communities. The account must have access to the whole Jive content that you want to index. You can use an existing administrator account but the best practice is to create a dedicated user with Full Access permissions.

**Example:** When Jive users create private documents, the crawling account must have Full Access permissions to allow the crawler to see these documents and index their content and associated permissions so that the owners and users authorized to see the private documents can see them in search results.

To create a Jive crawling account

1. Using an administrator account, with a browser, log in to the Jive Administration Console (http://[MyJiveCommunity]/admin).

2. When you want to create a dedicated crawling account:
   a. On the Jive Administration Console menu, select People > Management > Create User.
   b. In the Create User page, fill all the boxes to describing your crawling account, and then click Create User.
c. At the bottom of the User Summary page, click Save.

3. On the Jive Administration Console menu, select Permissions > System Administration.

4. In the System Administration Permissions page, in the Start typing to find a user box, type the name of your new or existing crawling account, select it, and then click Set override.

Note: Since the Jive REST API is not SSO-enabled, when your Jive instance is implemented with SSO, the crawling user you select must be a non-federated account (not an Active Directory user). Since it is not possible to authenticate against the REST API as a federated user, selecting such a user as the crawling account will return 401 status code errors. If the crawling account has already been set up as federated and changed to non-federated, the user has to be deleted and recreated (see 401 Unauthorized on .NET calls to v3 API).
In the Permissions for page, select the Full Access check box, and then click Set Permissions.

What's Next?

Optionally install the Coveo plugin used by the connector on your Jive server (see "Installing the Coveo Plugin on Your Jive Server" on page 1066).
9.21.6 Installing the Coveo Plugin on Your Jive Server

The Jive connector comes with an optional Coveo plugin that you can install on your Jive server to allow the Jive connector to access Jive features that are not available through the regular Jive 6+ APIs.

Note: You cannot install the Coveo plugin in Jive Cloud.

Plugin Benefits

The Jive connector can work without the plugin, but using the plugin enables the following connector features:

- Indexing permissions
- Indexing direct messages
- Removing recently deleted Jive items from the index during an incremental refresh

Note: CES 7.0.8691+ (December 2016) Removal of deleted Jive events.

- Proper incremental refresh of discussions
- Phrase substitutions

Important: The plugin stores deleted item information on the Jive server in a database to allow incremental refresh to remove deleted items from the index. The items in this database are cleared after they are read by the crawler. If no source is set to crawl the Jive site, the plugin database will grow indefinitely.

To install the Coveo plugin on your Jive server

1. Using an administrator account, with a browser, log in to the Jive Administration Console (http://[MyJiveCommunity]/admin).

2. On the Jive Administration Console menu, select System > Plugins > Add Plugin.

3. In the Available Plugins page:
a. Under **Install a new Plugin**, click **Choose File**.

b. Browse to the [CES_Path]\Bin\ folder on the Coveo Master server and using the following table, select the `coveo-plugin-[Version]-for-jive-[6.0/8-1.0].jar` plugin file corresponding to your Jive installation.

c. Click **Upload**.
4. Grant access to the Coveo plugin for the selected crawling account:

**Note:** By default, for security reasons, no accounts can connect to the Coveo for Jive plugin.

a. In the Administration Console, select **System > Management > System Properties**.

b. At the bottom of the **System Properties** page, in the **Add new property** box:

   ![Add new property form]

   i. In the **Property Name** box, enter `coveo.services.allowed.username`.
   
   ii. In the **Property Value** box, enter the user name of the selected crawling account.
   
   iii. Click **Save Property**.

5. Stop and restart the Jive service (from the command prompt: `/etc/init.d/jive-application restart`).

What's Next?

Create a user identity to hold the credentials of the Jive crawling account that you selected.

9.21.7 Configuring a Jive Security Provider

The Jive connector can index Jive 6+ permissions to ensure that in search results, users only see Jive content they are allowed to see directly in Jive.

When you choose to index permissions, the connector requires a security provider to resolve Jive user and group permissions and optionally to map them to Active Directory or Email identities.

When you do not want to index permissions, skip this section.
Notes:

- The security provider requires the Coveo for Jive plugin to be installed on the Jive server. If not already done, install the plugin (see "Installing the Coveo Plugin on Your Jive Server" on page 1066).

- You can get familiar with how Coveo components deal with permissions on documents both at indexing and query time.

- CES 7.0.7711+ (June 2015) Support for mapping Jive users to Email identities.

To configure a Jive security provider

1. On the Coveo server, access the Administration Tool.
3. In the navigation panel on the left, click Security Providers.
4. In the Security Providers page, click Add to create a new security provider.
5. In the Modify Security Provider page:
a. In the **Name** box, enter a name to identify this security provider.

   **Example:** Jive Security Provider

b. In the **Security Provider Type** drop-down list, select Jive (x64).

   **Note:** You should not confuse the Jive security provider with the Jive 5 / SBS / Clearspace security provider that must be used with Jive versions older than Jive 6.0.

c. In the **User Identity** section:

   i. In the drop-down list, select the user identity that you selected or created previously.

   ii. When needed, click **Add**, **Edit**, or **Manage user identities** respectively to create, modify, or manage user identities.

d. In the **Jive Server URL** box, enter your Jive server base address.

   **Example:** http://acme.community.com
Configure the interface to which the Jive security provider maps Jive users depending on your CES version:

- **CES 7.0.7711+ (June 2015)** In the **Security Provider** drop-down list, optionally select another security provider to allow the Jive security provider to map Jive accounts to another user type with which people are authenticated when they perform a search:
  
  o Select **(none)** when you do not want to map Jive users to another user type.
  
  o When the Jive LDAP is synchronized with an Active Directory, select the out-of-the-box **Active Directory** security provider to map Jive users to AD users.
  
  o When a primary email is defined for all users in Jive and they are authenticated with this email when they perform a search in your CES search interface, select the Email security provider you previously created (see Jive Connector Deployment Overview).

- **CES 7.0.7599– (April 2015)**

  i. (Optional) Select the **Map Jive Users to Active Directory Users** check box when you want Microsoft Windows users to be able to see Jive content in search results without having to log in with their Jive credentials in the search interface.

  Clear this option when you want to allow Jive users to search for Jive secured documents in a non Microsoft Windows environment. In this case, you also need to add the security provider to your Jive search interface to allow users to log in to Jive in the search interface to be able to see Jive secured documents in search results.

  **Note:** When this option is selected, permissions are stored in the index as Active Directory identities rather than as Jive identities.

  ii. When you select the **Map Jive Users to Active Directory Users** check box, in the **Security Provider for Jive User Mapping** section:

  A. In the drop-down list, select the **Active Directory** security provider that the Jive security provider will use to map Jive users and groups to Windows users and groups.

  B. When needed, click **Add, Edit, or Manage security providers** respectively to create, modify, or manage security providers.

f. (Optional) When you select the **Active Directory** security provider (**CES 7.0.7711+ (June 2015)**) or when you select the **Map Jive Users to Active Directory Users** check box (**CES 7.0.7599– (April 2015)**) in the previous step, you must also configure the following two parameters that work together to build the Windows identity from the Jive identity (otherwise leave the default values):

  A. In the **Regular Expression matching Jive Usernames** box, enter a regular expression that matches against Jive usernames. If you leave this box empty, the Windows identity will be a copy of the Jive identity.

    **Example:** The default value matches an email address and captures the part before the @ character:
    
    ```
    ([\w-\.]+)@((?:[\w]+\.)+)([a-zA-Z]{2,})
    ```

  B. In the **Replacement string for Active Directory Usernames** box, enter the pattern for Active
Directory identities using regular expression group substitutions in the \$[n] form.

The string \$1 stands for the first group captured by the regular expression specified in the Regular Expression matching Jive Usernames box, while \$2, \$3, etc. stand for subsequent groups.

**Example:** Your Jive and Windows identities are respectively in the MyName@MyCompany.com and MyCompany\MyName forms.

Enter \$2\$1 in the Replacement string for Active Directory Usernames parameter to build the Windows identities with a regular expression such as (\[\w-\.]\?\((\[\w]+\).\[a-zA-Z]+\)?(2,4) in the Regular Expression matching Jive Usernames parameter.

**g. CES 7.0.5556+ (June 2013)** Select the Jive Instance Allows Anonymous Access option when you want to map the Jive Everyone user to the Active Directory Everyone user. This check box is cleared by default.

**h. CES 7.0.8388+ (June 2016)** Select the Expand All Registered Users System Group option when you want the security provider to treat the All Registered Users group in Jive as a security group that needs to be expanded. This check box is cleared by default, meaning that All Registered Users is considered as a well-known group (containing all users of a Jive space). Consider selecting the option when you assign the group in item permissions.

**Note:** Selecting the option can impact the security cache performance if the number of group members increases rapidly.

When the group contains thousands of users, it is recommended to set the MaxAllowedTimeWithoutProgress hidden parameter to a large value (ex: 600 seconds) [see Hidden Parameter Section]. The default value is 300 seconds.

**i.** In the Security Group Cache Expiration Delay box, leave the default value (2 minutes) unless Coveo Support is instructing you to change it. This parameter sets the amount of idle time after which the crawler should flush its cache of security groups.

**j.** In the Parameters section, in rare cases the Coveo Support could instruct you to click Add Parameters to specify other security provider parameter names and values that could help to troubleshoot security provider issues.

**k.** Leave the Allow Complex Identities option cleared as it does not apply to this type of security provider.

**l.** Click Apply Changes.

What's Next?

Configure and index a Jive source (see "Configuring and Indexing a Jive Source" on page 1072).

9.21.8 Configuring and Indexing a Jive Source

A source defines a set of configuration parameters for a specific Jive 6+ server.

**Note:** In an environment with more than one Jive 6+ server, you need to define one source for each Jive server that you want to index.
To configure and index a Jive source

1. On the Coveo server, access the Administration Tool.

2. Select **Index > Sources and Collections**.

3. In the **Collections** section:
   a. Select an existing collection in which you want to add the new source.
   OR
   b. Click **Add** to create a new collection.

4. In the **Sources** section, click **Add**.

   The **Add Source** page that appears is organized in three sections.

5. In the **General Settings** section of the **Add Source** page:

   ![Add Source page](image)

   a. Enter the appropriate value for the following required parameters:

   **Name**

   Enter a descriptive name of your choice for the connector source.

   **Example:** Corporate Jive
Source Type

Select the connector used by this source. In this case, select Jive.

Notes:

- You should not confuse the Jive source with the Jive 5 / SBS / Clearspace source that must be used with Jive versions older than Jive 6.0.
- When you do not see Jive, your environment does not meet the requirements (see "Jive Connector Requirements" on page 1062).

Addresses

Enter the root address of the Jive server that you want to index.

Example: http://acme.community.com/

Refresh Schedule

Select the time interval at which the source is automatically refreshed to keep the index content up-to-date. The recommended Every day option instructs CES to refresh the source everyday at 12 AM.

Note: You can create new or modify existing source refresh schedules.

b. Review the value for the following parameters that often do not need to be modified:

Rating

Change this value only when you want to globally change the rating associated with all items in this source relative to the rating to other sources.

Example: When a source replaces a legacy system, you may want to set this parameter to High, so that in the search interface, results from this source appear earlier in the list compared to those from legacy system sources.

Document Types

If you defined a custom document type set for this source, select it.

Active Languages

If you defined custom active language sets, ensure to select the most appropriate for this source.

Fields

CES 7.0.8541+ (September 2016) Select the field set that you created earlier (see Jive Connector Deployment Overview).

Note: CES 7.0.8388– (June 2016) If you defined custom field sets, ensure to select the most appropriate for this source.

6. In the Specific Connector Parameters & Options section of the Add Source page:
When you use phrase substitutions in your Jive community (see the Jive document Substituting Phrases in the UI), you must set the following parameters. Otherwise, leave them blank.

**Locale used for phrase substitutions**

Enter the phrase substitution locale that the connector should use. The default locale is `default`, meaning that the actual machine locale is used.

Enter the locale in any of the following three formats:

- Language only (ex: `en`)
- Language and country (ex: `en_US`)
- Language, country, and variant (ex: `en_US_NY`)

**Theme used for phrase substitutions**

Enter the phrase substitution theme that the connector should use. The default theme is `custom`.

A metadata called `csPhraseSubstitution` will be available for use in the mapping file.

b. In the Metadata Mapping File box, enter the path to the mapping file that should apply to the items in this source (see "Creating and Using a Jive Mapping File" on page 1079).

When you remove the default mapping file (`[CES_Path]\Bin\Coveo.CES.CustomCrawler.Jive.Mappings.xml`) and leave this box empty, the connector maps no metadata to CES fields.

c. Select the type of Jive content to index using the following options:
Only retrieve published items

Select to only index Jive items for which the status is Published. Items with other statuses (such as Draft, Scheduled, Awaiting Moderation, Rejected, Abuse Hidden, Abuse Visible, Archived, Expired, Pending Approval, Deleted, Processing, Error, Unknown) are not indexed.

Notes:

- Incremental refresh catches Jive item status changes and respects the configuration of this parameter.
- (Jive 6 only) Retrieving unpublished content requires Jive 6 API 3.3+ on the Jive server. When the Jive API does not support retrieving unpublished content, you get the following message in the CES Console:

```
Retrieving unpublished content requires at least the version 3.3 of the Jive REST API to be installed on the Jive server. Please update your version (n.n) if you want to use this feature or check the 'OnlyIndexPublishedContent' option.
```

Index Communities content

Select to index the Jive communities and any item they contain. Selected by default.

Index Projects content

Select to index the Jive projects and any item they contain. Selected by default.

Index Social Groups content

Select to index the Jive social groups and any item they contain. Selected by default.

Index System Blogs content

Select to index the Jive system blogs and any item they contain. Selected by default.

Index User content

Select to index the user profiles, personal blogs, and private items (messages, documents and discussions). Not selected by default.
Notes:

- **CES 7.0.8541– (September 2016)** The option is selected by default.

- Permission changes in Jive for **User content** type cannot be updated in the index with incremental refresh like for other types of Jive content. When you want to index **User content**, keep permissions as up-to-date as possible in the index, and optimize the load to your Jive server, it is recommended to create a separate source for **User content** using parameters suggested in the following table.

<table>
<thead>
<tr>
<th>Source Options</th>
<th>Main source</th>
<th>Users content source</th>
</tr>
</thead>
<tbody>
<tr>
<td>Index Communities content</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Index Projects content</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Index Social Groups content</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Index System Blogs content</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Index Users content</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Refresh Schedule</td>
<td>Incremental (Every 5 minutes)</td>
<td>Full Refresh (Every day)</td>
</tr>
</tbody>
</table>

- **d.** Click **Add Parameter** when you want to show and change the value of advanced source parameters (see "Modifying Hidden Jive Source Parameters" on page 1081).

- **e.** The **Option** check boxes generally do not need to be changed:

  **Index Subfolders**

  This parameter is not taken into account for this connector.

  **Index the document's metadata**

  When selected, CES indexes all the document metadata, even metadata that are not associated with a field. The orphan metadata are added to the body of the document so that they can be searched using free text queries.

  When cleared (default), only the values of system and custom fields that have the **Free Text Queries** attribute selected will be searchable without using a field query.
Example: A document has two metadata:

- LastEditedBy containing the value Hector Smith
- Department containing the value RH

In CES, the custom field CorpDepartment is bound to the metadata Department and its Free Text Queries attribute is selected.

When the Index the document's metadata option is cleared, searching for RH returns the document because a field is indexing this value. Searching for hector does not return the document because no field is indexing this value.

When the Index the document's metadata option is selected, searching for hector also returns the document because CES indexed orphan metadata.

Document's addresses are case-sensitive

Leave the check box cleared. This parameter needs to be checked only in rare cases for systems in which distinct documents may have the same name but different casing.

Generate a cached HTML version of indexed documents

When you select this check box (recommended), at indexing time, CES creates HTML versions of indexed documents. In the search interfaces, users can then more rapidly review the content by clicking the Quick View link rather than opening the original document with the original application. Consider clearing this check box only when you do not want to use Quick View links or to save resources when building the source.

Open results with cached version

Leave this check box cleared (recommended) so that in the search interfaces, the main search result link opens the original document with the original application. Consider selecting this check box only when you do not want users to be able to open the original document but only see the HTML version of the document as a Quick View. In this case, you must also select Generate a cached HTML version of indexed documents.

7. In the Security section of the Add Source page, perform the following actions if the plugin was installed.
a. In the **Security Provider** drop-down list, when you chose to index Jive permissions, select the security provider that you created for this source (see “Configuring a Jive Security Provider” on page 1068).

   *Note: CES 7.0.8225+ (March 2016)* When you want to only index public Jive content, select **None**.

b. In the **Authentication** drop-down list, select the user identity that you created for the Jive community.

   *Note: CES 7.0.8225+ (March 2016)* When you want to only index public Jive content, select **None**.

c. Click **Save** to save the source configuration.

8. When you chose to not index Jive permissions, you can set source level permissions that apply to all documents in the source:

   a. In the navigation panel on the left, click **Permissions**.

   b. In the **Permissions** page, select **Specify the security permissions** to index.

   c. In the **Allowed Users** and **Denied Users** boxes, enter the users and groups that you respectively want to allow or deny to see search results from this source. The default is to allow **everyone** (Active Directory Group).

   d. Click **Apply Changes**.

9. When you are ready to start indexing the Jive source, click **Rebuild**.

10. Validate that the source building process is executed without errors:

    - In the navigation panel on the left, click **Status**, and then validate that the indexing proceeds without errors.

      OR

    - Open the CES Console to monitor the source building activities.

**What's Next?**

- Set an incremental refresh schedule for your source.
- Review possible known issues (see “Troubleshooting Jive Connector Issues” on page 1081).
- Consider modifying some hidden source parameters to try resolving other issues (see "Modifying Hidden Jive Source Parameters" on page 1081).

9.21.8.1 **Creating and Using a Jive Mapping File**

By default, the Jive connector uses the default mapping file ([CES Path]\Bin\Coveo.CES.CustomCrawler.Jive.Mappings.xml). When you want to customize how the connector maps Jive metadata to index fields, you can create a custom mapping file.

*Note: The Jive connector uses the standard mapping file schema to configure what metadata from your original Jive documents are associated with fields for the documents in the Coveo index.*

The first section of the mapping file, **CommonMappings**, defines fields that will apply to every document.
<?xml version="1.0" encoding="utf-8" ?>
<Mappings>
   <Version>1</Version>
   <CommonMapping>
      <Fields>
         <Field name="sysauthor">%[author.displayName]</Field>
         <!-- Jive system fields -->
         <Field name="syscstag">%[tags]</Field>
         <Field name="syscstaggroup">%[categories]</Field>
         <Field name="syscsplace">%[coveo.places.titles]</Field>
         <Field name="syscsplacetype">%[coveo.places.types]</Field>
      </Fields>
   </CommonMapping>

Example: The mapping <Field name="sysauthor">%[author.displayName]</Field> instructs the connector to copy the value of the author.displayName Jive metadata and paste it in the sysauthor Coveo index field for each indexed document.

The following sections of the Jive mapping file define fields for different types of Jive documents (file, space, direct message...).

Example: The fields for a Jive person type of documents are given in the following mapping file excerpt.

<Mapping type="person">
   <Title>%[displayName]</Title>
   <Body>%[displayName] %[emails(work).value] %[jive.profile[Title].value]</Body>
   <Fields>
      <Field name="UserProfile.FirstName">%[name.givenName]</Field>
      <Field name="UserProfile.LastName">%[name.familyName]</Field>
      <Field name="UserProfile.AccountName">%[jive.username]</Field>
      <Field name="UserProfile.Title">%[jive.profile[Title].value]</Field>
      <Field name="UserProfile.AboutMe">%[jive.profile[Biography].value]</Field>
      <Field name="UserProfile.PictureURL">%[thumbnailUrl]</Field>
      <Field name="UserProfile.WorkEmail">%[emails.work].value]</Field>
      <Field name="UserProfile.WorkPhone">%[phoneNumbers(work).value]</Field>
      <Field name="syslocation">%[location]</Field>
      <Field name="sysfiletype">causer</Field>
   </Fields>
</Mapping>

Note: The built-in mapping file includes only the standard Jive metadata, none of your Jive custom or business metadata. The connector however retrieves all metadata. If you create and assign to your Jive source a field set that includes field names that exactly match metadata names, they will be mapped automatically. It is therefore recommended to extend your Jive source field set to include matching fields for all useful metadata.

To create and use a custom mapping file

1. Using an administrator account, connect to the Coveo Master server.

2. Using a text editor:
   a. Create an XML file respecting the mapping file schema.

   Tip: You can use a copy of the default mapping file as a starting point.
b. Save the file using a name of your choice in the [Index_Path]\Config folder.

Example: C:\CES7\Config\MyJiveMapping.xml

3. Instruct the connector to use this mapping file for a given source by adding the path of the mapping file to the Mapping File source parameter (see “Configuring and Indexing a Jive Source” on page 1072).

9.21.8.2 Troubleshooting Jive Connector Issues

This topic describes general issues you may encounter while using the Jive connector and attempts to provide the best course of action to resolve them.

9.21.8.2.1 Incremental Refresh

Incremental refresh is not detecting modifications made to Jive permissions

Modifications made to permissions in Jive do not impact the last modification date of objects affected by the permission modification. Since incremental refresh is using this last modification date to retrieve objects to update, the permission modification is not detected.

When Jive permissions are frequently modified, schedule a daily CES security cache update to keep the index permissions synchronized with Jive permissions.

Incremental refresh is not retrieving items that were deleted more than two weeks ago

The connector needs to keep track of items that were deleted from Jive in order for incremental refresh to keep the index up-to-date. Every time an incremental refresh run completes, items that were deleted more than two weeks ago are removed from the deleted history.

If incremental refresh was disabled on a source for a period greater than two weeks and you have more than one source performing incremental refresh on the same Jive server, you should perform a source refresh on the source where incremental refresh was disabled to make sure your index is fully up-to-date.

9.21.8.3 Modifying Hidden Jive Source Parameters

The Add Source and Source: ... General pages of the Administration Tool present the parameters with which you can configure the connector for most Jive setups. More advanced and more rarely used parameters are hidden. You can choose to make one or more of these parameters appear in the Add Source and Source: ... General pages of the Administration Tool so that you can change their default value. Consider changing values of hidden parameters when you encounter issues.

The following list describes the advanced hidden parameters available with Jive 6 sources. The parameter type (Integer, String, Boolean) appears between parentheses following the parameter name.

IgnoreItemsOfTypes (String)

Semi-colon separated list of Jive item types to ignore while indexing. Possible values are: Announcement, Attachment, Checkpoint, Comment, Discussion, Dm, Document, File, Group, Idea, Message, Poll, Project, Space, SystemBlog, Task, Update, Video.

StartingSpaceUrl (String)

The URL of the space at which the crawling should start. Only content within this space and its subspaces will
be available in the index. This does not affect social groups and people.

**AdditionalHeaders (String)**  
List of headers that should be added to the web requests made by the connector in the following format: `key1=value1\;key2=value2`

**Example:** If you need to add a Web service authentication header with a key "User" and a value "CrawlingUser" you can enter the following string in this parameter: `user=CrawlingUser`

**IgnoreItemsOlderThan (String)**  
Specifies the modified date from which older items are not indexed. The date string must be in a format recognized by the Microsoft .NET Framework (see Standard Date and Time Format Strings). By default there are no dates and all items are indexed.

**RequestTimeout (Integer)**  
The maximum amount of time (in seconds) a request can be executed before being canceled. The default and optimal value is 100.

**BatchSize (Integer)**  
The number of items to retrieve with each call to Jive server. The default and optimal value is 25 items.

Use the following procedure only when you want to modify one or more of the above hidden source parameters.

**To modify hidden Jive source parameters**

1. Refer to "Adding an Explicit Connector Parameter" on page 450 to add one or more Jive hidden source parameters.

2. For a new Jive source, access the **Add Source** page of the Administration Tool to modify the value of the newly added advanced parameter:
   a. Select **Index > Sources and Collections**.
   b. Under **Collections**, select the collection in which you want to add the source.
   c. Under **Sources**, click **Add**.
   d. In the **Add Source** page, edit the newly added advanced parameter value.

3. For an existing Jive source, access the **Source: ... General** page of the Administration Tool to modify the value of the newly added advanced parameter:
   a. Select **Index > Sources and Collections**.
   b. Under **Collections**, select the collection containing the source you want to modify.
   c. Under **Sources**, click the existing Jive source in which you want to modify the newly added advanced parameter.
   d. In the **Source: ... General** page, edit the newly added advanced parameter value.

4. Rebuild your Jive source to apply the changes to the parameters.
9.22 Jive 5/SBS/Clearspace Connector

Deprecated

The Coveo connector for Jive 5, SBS, and Clearspace allows to index and integrate the content of your Jive, SBS and Clearspace communities into your Coveo unified index, making it easily searchable by end-users.

Note: The Jive 5/SBS/Clearspace connector was formerly known as the Jive connector. With the April 2013 monthly release, the new Jive connector must be used to index Jive 6+ content.

Features

The features of the Jive 5/SBS/Clearspace connector are:

- Content Indexing
  - The Jive connector retrieves and indexes following Jive object types:
    - Spaces (also known as Communities)
    - Projects (with related Tasks and Checkpoints)
    - User profiles
    - Social groups
    - Private messages
    - Documents (private and public)
    - Discussions (private and public)
    - Blog posts (for spaces, projects, users, social groups and system blogs)
    - Announcements
    - Polls
    - Comments (for documents, blog posts, and polls)
    - Attachments (for documents, blog posts, and discussions)
    - Tags and categories (formerly known as tag groups)
    - Phrase substitution

- Security
  - The connector indexes the permissions on Jive objects when the user and group names defined in Jive match entries in Microsoft Active Directory. Consequently, Coveo search results only contain Jive objects that the end-user can access within the Jive communities.

- Incremental refresh
  - The connector periodically queries Jive for the latest edits, keeping the index content up-to-date.
Feature history

<table>
<thead>
<tr>
<th>CES version</th>
<th>Release</th>
<th>Features</th>
</tr>
</thead>
<tbody>
<tr>
<td>7.0.5388+</td>
<td>April 2013</td>
<td>Connector renamed from Jive to Jive 5/SBS/Clearspace.</td>
</tr>
<tr>
<td>7.0.4855+</td>
<td>August 2012</td>
<td>• Can now manage phrase substitution&lt;br&gt;• New option to crawl only published documents</td>
</tr>
</tbody>
</table>

What's Next?

Get familiar with the deployment steps (see "Jive 5/SBS/Clearspace Connector Deployment Overview" on page 1084).

9.22.1 Jive 5/SBS/Clearspace Connector Deployment Overview

**Deprecated**

The following procedure outlines the steps needed to deploy the Jive 5/SBS/Clearspace connector. The steps indicate the order in which you must perform configuration tasks on both the Jive and Coveo servers.

1. **Validate that your environment meets the requirements** (see "Jive 5/SBS/Clearspace Connector Requirements" on page 1085).
2. **On the Jive server:**
   a. **Choose a crawling account**
      
      You must choose which Jive account the Coveo connector uses to crawl the content of your Jive communities. The account must have read access to the whole Jive content that you want to index. You can use an administrator account such as SysAdmin but the best practice is to create a dedicated user with full read permissions.
   b. **Enable the web services**
      
      You must ensure that the native Jive web services used by the Coveo connector are enabled on your Jive server (see "Enabling the Jive Web Services" on page 1085).
   c. **Upload the Coveo plugin**
      
      You must upload to your Jive server the Coveo plugin used by the connector (see "Uploading the Coveo Plugin on your Jive Server" on page 1087).
   d. **Configure authentication**
      
      With SBS 3 and Clearspace 2.5 installations only, you must configure your SBS/Clearspace server to allow .NET web service authentication (see "Configuring Authentication with Jive Web Services Using .NET" on page 1089).
3. **On the Coveo server:**
a. Create a user identity
You must enter in a user identity the credentials of the Jive crawling account that you selected (see "Adding a User Identity" on page 420).

b. Create a security provider
You must create security provider that the connector uses to map Jive users/groups to Microsoft Active Directory users/groups (see "Configuring a Jive 5/SBS/Clearspace Security Provider" on page 1089).

c. Create and index a source
You must create a source describing the Jive community to index (see "Configuring and Indexing a Jive 5/SBS/Clearspace Source" on page 1092).

d. Add support for CA SiteMinder
When your Jive server uses CA SiteMinder for user authentication, you need to add parameters to the connector (see "Adding CA SiteMinder Parameters to the Jive 5/SBS/Clearspace Connector" on page 1100).

4. Troubleshooting
   a. Review known cases (see "Troubleshooting Jive 5/SBS/Clearspace Connector Issues" on page 1102).
   b. Consider modifying some hidden source parameters to try resolving other issues (see "Modifying Hidden Jive 5/SBS/Clearspace Source Parameters" on page 1098).

9.22.2 Jive 5/SBS/Clearspace Connector Requirements

**Deprecated**
Your environment must meet the following requirements to be able to use the Coveo connector for Jive 5/SBS/Clearspace communities:

- **Coveo license for the Jive 5/SBS/Clearspace connector**
  Your Coveo license must include support for the Jive 5/SBS/Clearspace connector to be able to use this connector. You can see the currently supported connectors from the Administration Tool.

- **Supported Jive products**
  The Jive connector works with Jive 5.0, Jive SBS 4.5, SBS 4.0, SBS 3.0, and Clearspace 2.5 (2.5.5 and 2.5.7).

  **Note:** You need to use the new Jive connector to index Jive 6 content.

9.22.3 Enabling the Jive Web Services

**Deprecated**
The Jive 5/SBS/Clearspace connector uses the native Jive Web services to retrieve the content from the Jive communities. The Jive web services are disabled by default and must therefore be enabled in the Jive Administration Console.
To enable the web services in Jive

1. Using a browser, access the Jive Administration Console (using a URL in the http://[MyJiveCommunity]/admin).

2. In Administration Console, select **System > Settings > Web Services**.

3. In the **Web Services** page:

   a. Select **Enabled** for **Enable SOAP Web Services**.

   b. Under **User Access**, specify the Jive account that you chose to be used by the Coveo connector to crawl the Jive community content.

   c. Click **Save Settings**.
What's Next?

Upload to your Jive server the Coveo plugin used by the connector (see "Uploading the Coveo Plugin on your Jive Server" on page 1087).

9.22.4 Uploading the Coveo Plugin on your Jive Server

Jive has a plugin framework which can be used to call the Jive APIs. The Jive 5/SBS/Clearspace Coveo connector works with such a plugin to expose a custom web service that it uses to retrieve complementary information from Jive. You need to upload the Coveo plugin on your Jive server.

**Important:** When you are installing the plugin on a Jive server that was updated from Clearspace to SBS, before performing the following procedure, you must update the plugin database (see "Updating the Database Schema of the Coveo Plugin for Jive" on page 1088).

To upload the Coveo plugin on Jive server

1. Using a browser, access the Jive Administration Console (using a URL in the http://[MyJiveCommunity]/admin form).
2. In Administration Console, select **System > Plugins > Add Plugin**.
3. In the **Available Plugins** page:
a. Under **Install a new Plugin**, click **Choose File**.

b. **Browse to** the `[CES_Path]\Bin` folder on the Coveo Master server and select the `Coveo.CES.CustomCrawlers.Plugin.[Platform].jar` plugin file corresponding to your Jive installation.

<table>
<thead>
<tr>
<th>Jive installation</th>
<th>Plugin file</th>
</tr>
</thead>
<tbody>
<tr>
<td>Jive 5</td>
<td>Coveo.CES.CustomCrawlers.Clearspace.Plugin.SBS50.jar</td>
</tr>
<tr>
<td>Jive SBS 4.5</td>
<td>Coveo.CES.CustomCrawlers.Clearspace.Plugin.SBS45.jar</td>
</tr>
<tr>
<td>SBS 4.0</td>
<td>Coveo.CES.CustomCrawlers.Clearspace.Plugin.SBS40.jar</td>
</tr>
<tr>
<td>SBS 3.0</td>
<td>Coveo.CES.CustomCrawlers.Clearspace.Plugin.SBS30.jar</td>
</tr>
<tr>
<td>Clearspace 2.5</td>
<td>Coveo.CES.CustomCrawlers.Clearspace.Plugin.CS25.jar</td>
</tr>
</tbody>
</table>

c. Click **Upload**.

4. Stop and restart the Jive service (from the command prompt: `/etc/init.d/jive-application stop` and `/etc/init.d/jive-application restart`).

**What's Next?**

- With SBS 3 and Clearspace 2.5 installations only, configure your SBS/Clearspace server to allow .NET web service authentication (see "Configuring Authentication with Jive Web Services Using .NET" on page 1089).

  AND

- Create a user identity to hold the credentials of the Jive crawling account that you selected.

9.22.4.1 Updating the Database Schema of the Coveo Plugin for Jive

**Deprecated**

The Coveo plugin installed on the Jive server and used by the Jive 5/SBS/Clearspace connector creates a custom table on the Jive server database where it keeps track of deleted items. Following a server restart, this table is automatically created the first time the plugin is uploaded to the Jive server.

The definition of this table has been modified to support the SBS 4.0 platform. When your Jive server was updated from Clearspace 2.5 to SBS 4.0 and a Jive 5/SBS/Clearspace connector plugin for the Clearspace 2.5 platform was previously installed on that server, you may need to update the database. When this is the case, perform the following steps before you install the plugin for the SBS 4.0 platform.

To update the database schema of the Coveo plugin

1. Using an administrator account, connect to the Jive server.

2. Log on to the SBS server database.
3. Drop the coveoDeletedItems table.

4. Open the JiveVersion table and delete the coveoDeletedItems entry.

The new updated table named CESLiveIndexing will be available following a Jive server restart.

What's Next?

Upload the Coveo plugin on the Jive server (see "Uploading the Coveo Plugin on your Jive Server" on page 1087).

9.22.5 Configuring Authentication with Jive Web Services Using .NET

**Deprecated**

For the Jive 5/SBS/Clearspace connector, with Clearspace 2.5 and SBS 3.0 installations, you must configure the SBS server to allow .NET proxy classes to be able to authenticate with SBS web services. The following instructions were taken from a discussion on the Jive Developers Forum and were successfully tested with both Clearspace 2.5 and SBS 3.0 (see Generating Proxy Classes for Web Services).

To configure authentication with Jive web services using .NET

1. Using an administrator account, connect to the SBS server.

2. Stop the SBS service (from the command prompt: /etc/init.d/jive-application stop).

3. Locate the main Clearspace/SBS library file on the Jive server, generally located in the %SBSInstallationPath%/WEB-INF/lib/ folder. Depending on your platform, the library file will be named clearspace-2.5.X.jar or jive-sbs-public-3.0.X.jar.

4. Make a backup copy of this library file so you can revert any changes made at any time.

5. From the library, extract the spring-wsContext.xml file, and using a text editor:
   a. Open the spring-wsContext.xml file.
   b. Locate the following entry and remove NoSecurity from its value:

   ```
   <entry key="action" value="UsernameToken Timestamp NoSecurity" />
   ```
   c. Save the file.

6. Add the modified spring-wsContext.xml file into the library file, overwriting the original one.

7. Ensure that the Apache wss4j.jar file also located under WEB-INF/lib/ is the latest version. The Apache WSS4J file is available for download here.

8. Restart the SBS service (from the command prompt: /etc/init.d/jive-application restart).

9.22.6 Configuring a Jive 5/SBS/Clearspace Security Provider

**Deprecated**

The Jive 5/SBS/Clearspace connector needs a security provider to resolve mappings between users and groups defined in Jive and Microsoft Active Directory. The security provider is required even when your Jive server uses LDAP to perform user authentication.
To configure a Jive 5/SBS/Clearspace security provider

1. On the Coveo server, access the Administration Tool.
3. In the navigation panel on the left, click Security Providers.
4. In the Security Providers page, click Add to create a new security provider.
5. In the Modify Security Provider page:

   a. In the Name box, enter a name to identify this security provider.

      Example: Jive Security Provider
b. In the **Security Provider Type** drop-down list, select **Jive 5 / SBS / Clearspace (x64)**.

c. In the **User Identity** section:
   
i. In the drop-down list, select the user identity that you selected or created previously.
   
ii. When needed, click **Add, Edit, or Manage user identities** respectively to create, modify, or manage user identities.

d. In the **Active Directory Security Provider** section:
   
i. In the drop-down list, select the Active Directory security provider that the Jive security provider will use to map Jive users and groups to Windows users and groups.
   
ii. When needed, click **Add, Edit, or Manage security providers** respectively to create, modify, or manage security providers.

e. In the **Server Base URL** box, enter the base address of the Jive server.

   **Example:** http://JiveWebSite:8080/Jive

f. In the **Users Cache Directory** box, enter the folder where the user cache files are saved. Jive users are saved in a local cache on the Coveo server to improve performances on large Jive communities.

   **Example:** C:\Temp

g. In the **LDAP Search Root** box, enter the LDAP root address under which the security provider attempts to find Jive users.

   **Example:** LDAP://OU=JIVE,DC=CORP, DC=DOMAIN, DC=COM

h. In the **LDAP Username** box, enter the username to use to authenticate with LDAP.

   **Note:** The LDAP credentials are only required when the Windows Identity under which CES is running is not from the same domain as the Jive users.

i. In the **LDAP Password** box, enter the password to use to authenticate with LDAP.

j. In the **Users Cache Life Span** box, consider changing the time interval between user cache refreshes, determining the cache validity period. Any value in minutes. The default is 1440 minutes (24 hours).

k. In the **Parameters** section, in rare cases the Coveo Support could instruct you to click **Add Parameters** to specify other security provider parameter names and values that could help to troubleshoot security provider issues.

l. Leave the **Allow Complex Identities** option cleared as it does not apply to this type of security provider.

m. Click **Apply Changes**.

What's Next?

Configure and index a Jive source (see "Configuring and Indexing a Jive 5/SBS/Clearspace Source" on page 1092).
9.22.7 Configuring and Indexing a Jive 5/SBS/Clearspace Source

Deprecated

A source defines a set of configuration parameters for a specific Jive 5/SBS/Clearspace server.

**Note:** In an environment with more than one Jive 5/SBS/Clearspace server, you need to define one source for each Jive 5/SBS/Clearspace server that you want to index.

To configure and index a Jive 5/SBS/Clearspace source

1. On the Coveo server, access the Administration Tool.
2. Select Index > Sources and Collections.
3. In the Collections section:
   a. Select an existing collection in which you want to add the new source.
   OR
   b. Click Add to create a new collection.
4. In the Sources section, click Add.

The Add Source page that appears is organized in three sections.

5. In the General Settings section of the Add Source page:
a. Enter the appropriate value for the following required parameters:

Name

Enter a descriptive name of your choice for the connector source.

Example: Corporate Jive

Source Type

CES 7.0.7814+ (August 2015) Select the connector used by this source. In this case, select Jive 5 / SBS / Clearspace (deprecated).

Notes:

- If you do not see Jive 5 / SBS / Clearspace (deprecated), your environment does not meet the requirements (see "Jive 5/SBS/Clearspace Connector Requirements" on page 1085).

Addresses

Enter the root address of the Jive community from which to start indexing in the form:

http://[JiveserverName]:[port]/

where you replace [JiveserverName]:[port] by the host name and port of your Jive community. The default port is 8080. The port is optional when equal to 80.

Example: To index:

- All communities: http://JiveSite:8080/
- Community A: http://JiveSite:8080/ CommunityA
- Community C: http://JiveSite:8080/CommunityA/CommunityB/CommunityC

Refresh Schedule

Select the time interval at which the source is automatically refreshed to keep the index content up-to-date. The recommended Every day option instructs CES to refresh the source everyday at 12 AM.

Note: You can create new or modify existing source refresh schedules.

b. Review the value for the following parameters that often do not need to be modified:

Rating

Change this value only when you want to globally change the rating associated with all items in this source relative to the rating to other sources.

Example: When a source replaces a legacy system, you may want to set this parameter to High, so that in the search interface, results from this source appear earlier in the list compared to those from legacy system sources.
**Document Types**

If you defined a custom document type set for this source, select it.

**Active Languages**

If you defined custom active language sets, ensure to select the most appropriate for this source.

**Fields**

If you defined custom field sets, ensure to select the most appropriate for this source.

6. In the **Specific Connector Parameters & Options** section of the **Add Source** page:

![Specific Connector Parameters & Options](image)

   a. The following parameters generally do not need to be changed:

   **Number of Refresh Threads**

   Enter the number of simultaneous downloads handled by the connector. The default value is 2.

   **Theme used for phrase substitutions**

   When you use phrase substitutions in your Jive community (see the Jive document [Substituting Phrases in the UI](#)), enter the phrase substitution theme that the connector should use, and then select the **Use Phrase Substitutions** check box. The default theme is `custom`. This parameter is available with CES 7.0.4855+.
Locale used for phrase substitution

When you use phrase substitutions in your Jive community (see the Jive document Substituting Phrases in the UI), enter the phrase substitution locale that the connector should use, and then select the Use Phrase Substitutions check box. The default locale is default, meaning that the actual machine locale is used. This parameter is available with CES 7.0.4855+.

Enter the locale in any of the following three formats:

- Language only (ex: en")
- Language and country (ex: en_US)
- Language, country, and variant (ex: en_US_NY)

b. Select the type of Jive content to index using the following options:

Only retrieve published items

Select to only index Jive items for which the status is Published. Items with other statuses (such as Draft, Scheduled, Waiting Moderation, Rejected, Abuse Hidden, Abuse Visible, Archived, Expired, Pending Approval, Deleted, Processing, Error, Unknown) are not indexed. This parameter is available with CES 7.0.4855+.

Note: Incremental refresh catches Jive item status changes and respects the configuration of this parameter.

Use phrase substitutions

Select to index phrase substitutions. The substituted value is saved in the csPhraseSubstitution field for each document. This parameter is available with CES 7.0.4855+.

Note: The default phrase substitution feature is designed for an English user interface. When your Jive community includes user interfaces in other languages with phrase substitutions for localized names, the connector cannot directly index these substitutions.

Example: When you are using a French interface, Space is called Espace. If you add a phrase substitution for Espace", the connector searches for Space and does not find it.

You can use advanced source parameters to provide a pattern to search for the specific item type (see "PhraseSubstitutionsAnnouncementPattern (String)" on page 1099).

Index Communities content

Select to index the Jive communities and any item they contain. Selected by default.

Index Projects content

Select to index the Jive projects and any item they contain. Selected by default.

Index Social Groups content

Select to index the Jive social groups and any item they contain. Selected by default.
Index System Blogs content

Select to index the Jive system blogs and any item they contain. Selected by default.

Index User content

Select to index the user profiles, personal blogs, and private items (messages, documents and discussions). Selected by default.

c. Click Add Parameter when you want to show and change the value of advanced source parameters (see "Modifying Hidden Jive 5/SBS/Clearspace Source Parameters" on page 1098).

d. The Option check boxes generally do not need to be changed:

Index Subfolders

Keep this check box selected (recommended). By doing so, to recursively index all communities found under the community specified in Addresses.

Index the document's metadata

When selected, CES indexes all the document metadata, even metadata that are not associated with a field. The orphan metadata are added to the body of the document so that they can be searched using free text queries.

When cleared (default), only the values of system and custom fields that have the Free Text Queries attribute selected will be searchable without using a field query.

Example: A document has two metadata:

- LastEditedBy containing the value Hector Smith
- Department containing the value RH

In CES, the custom field CorpDepartment is bound to the metadata Department and its Free Text Queries attribute is selected.

When the Index the document's metadata option is cleared, searching for RH returns the document because a field is indexing this value. Searching for hector does not return the document because no field is indexing this value.

When the Index the document's metadata option is selected, searching for hector also returns the document because CES indexed orphan metadata.

Document's addresses are case-sensitive

Leave the check box cleared. This parameter needs to be checked only in rare cases for systems in which distinct documents may have the same name but different casing.

Generate a cached HTML version of indexed documents

When you select this check box (recommended), at indexing time, CES creates HTML versions of indexed documents. In the search interfaces, users can then more rapidly review the content by clicking the Quick View link rather than opening the original document with the original application. Consider clearing this check box only when you do not want to use Quick View links or to save
resources when building the source.

**Open results with cached version**

Leave this check box cleared (recommended) so that in the search interfaces, the main search result link opens the original document with the original application. Consider selecting this check box only when you do not want users to be able to open the original document but only see the HTML version of the document as a Quick View. In this case, you must also select *Generate a cached HTML version of indexed documents*.

7. In the **Security** section of the **Add Source** page:
   
   ![Security page screenshot]

   a. In the **Security Provider** drop-down list, select the security provider that you created for this source (see "Configuring a Jive 5/SBS/Clearspace Security Provider" on page 1089).
   
   b. In the **Authentication** drop-down list, select the user identity that you created for the Jive community.
   
   c. Click **Save** to save the source configuration.

8. In the navigation panel on the left, click **General**. In the **General** page:
   
   a. Modify the **Title Selection Sequence** so that **Use the filename** is the first option from the list.
   
   b. Click **Apply Changes**.

9. When you are ready to start indexing the Jive 5/SBS/Clearspace source, click **Rebuild**.

10. Validate that the source building indexing process is executed without errors:

    - In the navigation panel on the left, click **Status**, and then validate that the indexing proceeds without errors.
      
      OR
      
      - Open the CES Console to monitor the source building activities.

What's Next?

Set an incremental refresh schedule for your source.

When your Jive 5/SBS/Clearspace server uses CA SiteMinder for user authentication, add parameters to the connector (see "Adding CA SiteMinder Parameters to the Jive 5/SBS/Clearspace Connector" on page 1100).
9.22.7.1 Modifying Hidden Jive 5/SBS/Clearspace Source Parameters

**Deprecated**

The **Add Source** and **Source: ... General** pages of the Administration Tool present the parameters with which you can configure the connector for most Jive 5/SBS/Clearspace setups. More advanced and more rarely used parameters are hidden. You can choose to make one or more of these parameters appear in the **Add Source** and **Source: ... General** pages of the Administration Tool so that you can change their default value. Consider changing values of hidden parameters when you encounter issues.

The following list describes the advanced hidden parameters available with Jive 5/SBS/Clearspace sources. The parameter type (Integer, String, Boolean) appears between parentheses following the parameter name.

**ServiceTimeout (Integer)**

The time the connector waits for a web service request to complete. Any value in seconds. The default is 120 seconds.

**ServiceBatchSize (Integer)**

The number of items to retrieve in a single call to the Jive web services. The default value is 25.

**UserCacheLifeSpan (Integer)**

The connector keeps a local cache of all the Jive users. This way the connector does not have to retrieve all users from Jive on every full or incremental refresh run. This parameter controls the amount of time (in minutes) this user cache remains valid. When this delay expires, all users are fetched again, instead of being taken out of the cache. The default value is 1440 minutes (24 hours).

**ItemTypesToIgnore (String)**

List of Jive item types to ignore while indexing. Possible values are: Announcement, Blog, Discussion, Document, Poll, ProjectCheckPoint, ProjectTask, PrivateMessage

**DownloadUserProfilePictures (Boolean)**

When set to true, the connector downloads the images associated with each user profile and adds them as thumbnails to the CES documents.
PhraseSubstitutionsAnnouncementPattern (String)
PhraseSubstitutionsBlogPattern (String)
PhraseSubstitutionsCheckpointPattern (String)
PhraseSubstitutionsCommentPattern (String)
PhraseSubstitutionsCommunityPattern (String)
PhraseSubstitutionsDirectMessagePattern (String)
PhraseSubstitutionsDiscussionPattern (String)
PhraseSubstitutionsDocumentPattern (String)
PhraseSubstitutionsMessagePattern (String)
PhraseSubstitutionsPollPattern (String)
PhraseSubstitutionsPrivateMessagePattern (String)
PhraseSubstitutionsProjectPattern (String)
PhraseSubstitutionsSocialGroupPattern (String)
PhraseSubstitutionsSystemBlogPattern (String)
PhraseSubstitutionsTaskPattern (String)
PhraseSubstitutionsUserPattern (String)

**CES 7.0.4855+ (August 2012)** When your Jive community includes a non-English user interface with phrase substitutions for localized names and the **Use phrase substitutions** source option is selected, the connector cannot directly index these substitutions. Use these parameters to provide a pattern to search for the specific item type. The default value for the above parameters are respectively: Announcement, Blog, Checkpoint, Comment, Space, Direct Message, Discussion, Document, Message, Poll, Private Message, Project, Social Group, System Blog, Task, and User.

**Example:** When you are using a French interface, Space is called Espace. If you add Communauté as a phrase substitution for Espace, add the PhraseSubstitutionsCommunityPattern source parameter with the value Espace to allow the connector to index the phrase substitution for the item type.

Use the following procedure only when you want to modify one or more of the above hidden source parameters.

**To modify hidden Jive 5/SBS/Clearspace source parameters**

1. Refer to "Adding an Explicit Connector Parameter" on page 450 to add one or more Jive 5/SBS/Clearspace hidden source parameters.

2. For a new Jive 5/SBS/Clearspace source, access the Add Source page of the Administration Tool to modify the value of the newly added advanced parameter.
a. Select **Index > Sources and Collections**.

b. Under **Collections**, select the collection in which you want to add the source.

c. Under **Sources**, click **Add**.

d. In the **Add Source** page, edit the newly added advanced parameter value.

3. For an existing Jive 5/SBS/Clearspace source, access the **Source: ... General** page of the Administration Tool to modify the value of the newly added advanced parameter:

a. Select **Index > Sources and Collections**.

b. Under **Collections**, select the collection containing the source you want to modify.

c. Under **Sources**, click the existing Jive 5/SBS/Clearspace source in which you want to modify the newly added advanced parameter.

d. In the **Source: ... General** page, edit the newly added advanced parameter value.

4. Rebuild your Jive 5/SBS/Clearspace source to apply the changes to the parameters.

---

### 9.22.8 Adding CA SiteMinder Parameters to the Jive 5/SBS/Clearspace Connector

**Deprecated**

When the Jive 5/SBS/Clearspace server that you want to index uses CA SiteMinder to perform user authentication, you must add parameters to the Jive 5/SBS/Clearspace connector to support communications with the Jive web services.

To add CA SiteMinder parameters to the Jive 5/SBS/Clearspace connector

1. Identify the complete URL to the SiteMinder form login page, also known as the Forms Credential Collector (FCC).

   **Example:** `https://www.MyJiveServer.com/siteminderagent/forms/login.fcc`

2. Identify the POST action of the SiteMinder FCC, which is the text string that is submitted when a login attempt is made.

   The text string is a concatenation of the field ID and value pair of some of the fields from the FCC presented in the following table.

<table>
<thead>
<tr>
<th>Field Id</th>
<th>Field Value</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>USER</td>
<td>User name used to authenticate with SiteMinder.</td>
<td>jdow</td>
</tr>
<tr>
<td>PASSWORD</td>
<td>Password used to authenticate with SiteMinder.</td>
<td>qwerty</td>
</tr>
</tbody>
</table>
Coveo Platform 7.0 | Administrator Guide

<table>
<thead>
<tr>
<th>Field Id</th>
<th>Field Value</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>SMAUTHREASON</td>
<td>The code associated with a login failure.</td>
<td>Always use 0 (zero)</td>
</tr>
<tr>
<td></td>
<td>inspect the source code of the FCC. This URL must be escaped.</td>
<td></td>
</tr>
</tbody>
</table>

**Example:** USER=jdow&PASSWORD=qwerty&SMAUTHREASON=0 &TARGET=https%3A%2F%2Fwww.acme.com%2authenticate.aspx

3. On the Coveo server, access the Administration Tool.
4. In the Administration Tool, select **Configuration > Connectors**.
5. In the Connectors page, click **Jive 5 / SBS / Clearspace**.
6. In the **Jive 5 / SBS / Clearspace Connector** page, click **Add Parameter**.
7. In the **Modify the parameters of the additional connector** page:

![Image of the Administration Tool page](image-url)
a. For each parameter specified in the following table, enter the parameter information.

<table>
<thead>
<tr>
<th>Type</th>
<th>Name</th>
<th>Default Value</th>
<th>Label</th>
<th>Option</th>
</tr>
</thead>
<tbody>
<tr>
<td>String</td>
<td>SiteMinderFormLoginAction</td>
<td>The complete URL to the SiteMinder FCC</td>
<td>SiteMinder Form Login Action</td>
<td>Optional parameter</td>
</tr>
<tr>
<td>String</td>
<td>SiteMinderFormLoginPage</td>
<td>The POST action of the SiteMinder FCC</td>
<td>SiteMinder Form Login Page</td>
<td>Optional parameter</td>
</tr>
</tbody>
</table>

b. Click **Save**.

9.22.9 Troubleshooting Jive 5/SBS/Clearspace Connector Issues

**Deprecated**

The following sections describe general issues you may encounter while using the Jive 5/SBS/Clearspace connector and attempts to provide the best course of action to resolve them.

9.22.9.1 Group Permissions

**Changes to some group permissions within Jive are not effective in CES, even after security the cache was updated**

Permissions in Jive are flexible. They support users and groups, use inheritance to propagate through sub-communities, and support a hierarchy of precedence so an explicit permission always overrides an inherited one, whether it is denied or allowed.

Since permissions in CES only support denied and allowed entries, a denied entry always overrides an allowed entry for a user or a group, with no regard to whether the allowed permission was inherited or explicitly set. For that reason, when group permissions are used in Jive, in some cases these groups have to be expanded and permissions have to be set on group members to make sure CES permissions mirror those from Jive.

**Example:** Consider the following situation.

**Group A contains three members:** member 1, member 2 and member 3.

For a given Jive community, Group A is denied the View Documents permission through an inherited permission but member 1 is explicitly allowed the View Document permission.

When you look at the final permissions in CES, you see that member 1 is effectively allowed on any document from that community and that member 2 and member 3 are denied. There will be no denied permission set on Group A since doing so would deny all members from the group, including member 1.

Therefore, expanding groups and setting permissions on group members rather than on the groups themselves is not effective in CES until a refresh operation is performed.
9.22.9.2 Incremental Refresh

**Incremental refresh is not detecting modifications made to Jive permissions**

Modifications made to permissions in Jive do not impact the last modification date of objects affected by the permission modification. Since incremental refresh is using this last modification date to retrieve objects to update, the permission modification is not detected.

When Jive permissions are frequently modified, schedule a source refresh weekly or more often to keep the index permissions synchronized with Jive permissions.

**Incremental refresh is not detecting new users added to the Jive server**

The Jive 5/SBS/Clearspace connector keeps a local cache of all active Jive users for faster access and to improve indexing performances. New Jive users are detected by incremental refresh and added to CES only when this local cache of users expires and is refreshed.

By default, the user cache is refreshed every 24 hours but can be refreshed more often by adding the UserCacheLifeSpan parameter to your source and setting its value (in minutes) accordingly (see "Modifying Hidden Jive 5/SBS/Clearspace Source Parameters" on page 1098).

**Note:** The UserCacheLifeSpan parameter is also available on the security provider and its value should always match the value set on its associated source (see "Configuring a Jive 5/SBS/Clearspace Security Provider" on page 1089). If a security provider is used by more than one source, make sure the UserCacheLifeSpan parameter on the security provider matches the lowest value of this parameter among all its associated sources.

**Incremental refresh is not retrieving items that were deleted more than two weeks ago**

The connector needs to keep track of items that were deleted from Jive in order for incremental refresh to keep the index up-to-date. Every time a incremental refresh run completes, items that were deleted more than two weeks ago are removed from the deleted history.

If incremental refresh was disabled on a source for a period greater than two weeks and you have more than one source performing incremental refresh on the same Jive server, you should perform a source refresh on the source where incremental refresh was disabled to make sure your index is fully up-to-date.

9.22.9.3 Secure Addresses

When clicking on search results within a CES search page, you are taken to a secure Jive connection (e.g.: https://JiveSite:8443/docs/DOC-1001) even though the starting address specified on the source is not (e.g.: http://JiveSite:8080)

If the web server hosting Jive is configured so that SSL is enabled for Jive, you should always use the secure starting address.

9.22.9.4 Error during Refresh or Rebuild

When refreshing or rebuilding a Jive source, the following error is displayed and the operation is aborted:

Jive Error: Client found response content type of 'text/html;charset=ISO-8859-1', but
expected 'text/xml'. The request failed with the error message:
```
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.0 Transitional//EN">
<html><head><title>System Error</title></head>
<body><div id="jive-header" class="jive-clearfix">
<h1>System Error</h1></div><p>We're sorry but a serious error has occurred in the system.
This is the typical error message returned by Jive when an internal error occurs on the Jive server. While there is not much that you can do to prevent these errors from occurring, it is recommended to restart the Jive service if the errors occur frequently.

When refreshing or rebuilding a Jive source, the following error is displayed and the operation is aborted:

Jive Error: PermGen space.

A PermGen related error means the Jive server was temporarily out of memory. If this error occurs repeatedly, ensure your Jive JVM settings follow the recommendation and, if required, increase the PermGen Heap space to at least 512 MB (see the Jive document Adjusting the Java Virtual Machine (JVM) Settings).

9.23 Liferay Connector

The Coveo beta connector for Liferay portals allows crawling and bringing Liferay content into the unified index, making it easily searchable by end-users.

9.23.1 Features

The following details the features available in the Liferay connector:

**Content indexing**

The connector can retrieve and index exclusively the following default Liferay portal entity types:

- Communities
- Organizations
- Users
- User groups
- Blogs
- Calendar events
- Document libraries
- Message boards
- Web content
- Wikis
- Comments and files attached to indexed entity types.
The connector can be customized to index other default Liferay entities (see "Customizing the Liferay Connector Mapping File" on page 1124).

Fully supported security model

The connector fully supports the Liferay security model using a security provider to get permissions for each indexed Liferay item. This means that, in Coveo search interfaces, a user searching Liferay content only sees the content to which he has access in the Liferay portal.

Partial incremental refresh

The Coveo Liferay portlet plugin registers events to quickly and efficiently index new, modified, and deleted Liferay items.

Note: Some item changes require a source full refresh to be taken into account (see Limitations).

9.23.2 Limitations

- Limited incremental refresh capabilities:
  - A full refresh is needed to update permission changes.
  - A full refresh is needed to update Wiki page attachment changes.
  - A full refresh is needed to update moved items.

9.23.3 Feature History

<table>
<thead>
<tr>
<th>CES version</th>
<th>Date</th>
<th>Features</th>
</tr>
</thead>
<tbody>
<tr>
<td>7.0.8047</td>
<td>December 2015</td>
<td>Support for Liferay 6.1</td>
</tr>
<tr>
<td>7.0.5388</td>
<td>April 2013</td>
<td>Support of permission levels and sets.</td>
</tr>
</tbody>
</table>

What's Next?

Review the deployment process (see "Liferay Connector Deployment Overview" on page 1105).

9.23.4 Liferay Connector Deployment Overview

The following procedure outlines the steps needed to deploy the Liferay connector. The steps indicate the order in which you must perform configuration tasks on both the Liferay and Coveo servers.

1. Validate that your environment meets the requirements (see "Liferay Connector Requirements" on page 1107).

2. In Liferay:
   a. Deploy the Coveo Liferay portlet plugin.

      The Coveo connector communicates with this plugin to crawl and index the Liferay content (see "About the Coveo Liferay Portlet Plugin Deployment" on page 1108).
b. Select or create the crawling account.

The Coveo connector needs a Liferay account with which it can fully crawl the Liferay content (see “Setting up a Liferay Crawling Account” on page 1114).

3. In the Coveo Administration Tool:

   a. Configure a user identity.

      The Coveo connector needs to know the Liferay account that you previously selected or created (see “Setting up a Liferay Crawling Account” on page 1114). You must create a CES user identity to use this account. Use either the Screen Name or the Email Address of the dedicated Liferay account (see “Adding a User Identity” on page 420). You will later assign this user identity to the security provider and the source used by the connector to crawl the Liferay content (see “Configuring and Indexing a Liferay Source” on page 1118).

b. **CES 7.0.8047+ (December 2015)** Optionally create security providers.

   When you want to index Liferay permissions, you need at least two security providers to get Liferay item permissions and resolve and expand groups.

   In Liferay, users are identified by their screen names. Consequently, permissions returned by the Liferay security provider for each document are screen names (may be expanded from groups). The Liferay security provider then requires another security provider to uniquely identify users from their screen names.

   i. Start by selecting or creating a security provider that the Liferay security provider will use to resolve and expand groups. The security provider type to use depends on how users are authenticated when they access the search interface:

      - When authenticated with their Active Directory (AD) user logon name, which match their screen name in Liferay, use the out-of-the-box or create a custom Active Directory security provider (see “Configuring an Active Directory Security Provider” on page 1141).

      - When authenticated with their Active Directory (AD) account in the DOMAIN\username format, use a REGEX Transform Member Name security provider chained to an Active Directory security provider to map the two member types (see “Configuring an Active Directory Security Provider” on page 1141 and “Configuring a REGEX Transformation Security Provider” on page 67).

        **Important:** A regex rule must be able to transform the Liferay screen name, so that the screen name match the AD username. Contact Coveo Support for assistance.

      - When authenticated with their email address, use a REGEX Transform Member Name security provider chained to an Email security provider to map the two member types (see “Configuring an Email Security Provider” on page 65 and “Configuring a REGEX Transformation Security Provider” on page 67).

        **Important:** A regex rule must be able to transform the Liferay screen name, so that the screen name match the email address. Contact Coveo Support for assistance.
ii. Then create a Liferay security provider chained with the security provider(s) you just created that the connector uses to resolve indexed permissions (see "Configuring a Liferay Security Provider" on page 1116).

Note: CES 7.0.7914– (October 2015) You need to configure a Liferay security provider, and then add the security provider on your .NET search interface since you cannot map Liferay user identities to AD ones (see "Configuring a Liferay Security Provider" on page 1116 and "Adding Security Providers to a .NET Search Interface" on page 631).

Important: JavaScript search interfaces cannot contain secured Liferay content.

c. Configure and index the Liferay source

The Coveo connector needs to know details about the Liferay portal to be able to index its content (see "Configuring and Indexing a Liferay Source" on page 1118).

d. Optionally, customize the mapping file to fine-tune indexed content

Consider customizing the connector mapping file to fine-tune the indexed content or to index other entities in your Liferay portal (see "About the Liferay Connector Mapping File" on page 1123 and "Customizing the Liferay Connector Mapping File" on page 1124).

e. Optionally, modify hidden source parameters

Once your Liferay source is up and running, if you encounter issues, consider modifying some hidden source parameters to try resolving the issues (see "Modifying Hidden Liferay Source Parameters" on page 1125).

4. In the Interface Editor, add the built-in Liferay facets

CES comes with a built-in Liferay Type facet that you can add to your search interface so that users can more easily refine search results based on file types (see "Managing Built-in Facets and Related Results Appearing in a .NET Search Interface" on page 574).

9.23.5 Liferay Connector Requirements

Your environment must meet the following requirements to be able to use the Coveo connector for Liferay portals:

- Coveo license for the Liferay connector
  
  Your Coveo license must include support for the Liferay connector to be able to use this connector.

- Liferay version 6 or 6.1
  
  The connector was developed and tested with Liferay version 6.0.5.

Note: CES 7.0.8047+ (December 2015) Support for Liferay 6.1.

What's Next?

Review the deployment process (see "Liferay Connector Deployment Overview" on page 1105).
9.23.6 About the Coveo Liferay Portlet Plugin Deployment

The Coveo connector retrieves content from the Liferay portal by connecting to the Coveo Liferay portlet plugin. You must deploy the plugin on the Liferay server.

Depending on your Liferay version:

- "Deploying the Coveo Liferay Portlet Plug-in for Liferay 6.0" on page 1108
- "Deploying the Coveo Liferay Portlet Plug-in for Liferay 6.1" on page 1111

9.23.6.1 Deploying the Coveo Liferay Portlet Plug-in for Liferay 6.0

You must install the version 6.0.6.1 of the Coveo plugin for Liferay on your Liferay server to index Liferay 6.0 content.

Note: CES 7.0.7914–(October 2015) You must install the 6.0.5.1 version of the plugin.

To deploy the Coveo Liferay portlet plugin

1. Using an administrator account, connect to the Coveo server.
2. From a browser, use an administrator account to connect to your Liferay portal.
3. On the menu bar of the Liferay portal, select Manage > Control Panel.
4. In the Liferay Control Panel:

   a. In the navigation panel on the left, under Server, click Plugins Installation.
   b. In the Plugins Installation page, select Portlet Plugins, and then click Install More Portlets.
   c. In the Plugin Installer page:
i. Select **Upload File**.

ii. Click **Choose File**, and then browse to and select the Coveo Liferay portlet plugin Web archive (WAR) file: 

```
[CES_Path]\bin\CESLiferayConnector-portlet-6.0.6.1.war
```

**Example:** With the default installation path:

```
C:\Program Files\Coveo Enterprise Search 7\bin\CESLiferayConnector-portlet-6.0.6.1.war
```

iii. Click **Install**.

**d.** End-users do not need to see the Coveo portlet. Consider hiding the Coveo portlet from users other than Administrator role members:

i. In the navigation panel on the left, under **Portal**, select **Plugins Configuration**.

ii. In the **Plugins Configuration** page, select the **CES Liferay Connector by Coveo Solutions Inc.** plugin.

iii. Under **Permissions**, for each user other than Administrator, click **Change**.
iv. In the Roles page, clear the Add to page check box, and then click Save.

v. Navigate back to the Plugins Configuration page for the Coveo plugin, and then click Save.

5. You must also enable access to the Liferay Web services for the Coveo server:

   a. Using an administrator account, connect to the Liferay server.

   b. Using a text editor:
      
      i. Open, or create if it does not already exist, the [Liferay_Installation_Path]\tomcat-x.x.xx\webapps\ROOT\WEB-INF\classes\portal-ext.properties text file.

      ii. Add the following lines to the file to allow access only to the Coveo Master server:

```
axis.servlet.hosts.allowed=[Coveo_Server_IP_Address]
axis.servlet.https.required=false
tunnel.servlet.hosts.allowed=[Coveo_Server_IP_Address]
tunnel.servlet.https.required=false
```

where you replace [Coveo_Server_IP_Address] by the IP address of the Coveo Master server.

   iii. Restart the Liferay server to apply changes to the properties and activate the listeners used for incremental refresh by shutting down and restarting the Web server:
Example: With a Tomcat server, in a command prompt window, run the following files:

C:\liferay-portal-6.0.6\tomcat-6.0.29\bin\shutdown.bat
C:\liferay-portal-6.0.6\tomcat-6.0.29\bin\startup.bat

Restarting the server is required to apply changes to the properties and activate the listeners used for incremental refresh.

What's Next?

Create a Liferay account with which the Coveo connector can fully crawl the Liferay content (see "Setting up a Liferay Crawling Account" on page 1114).

9.23.6.2 Deploying the Coveo Liferay Portlet Plug-in for Liferay 6.1

CES 7.0.8047+ (December 2015)

You must install the version 6.1.1.1 of the Coveo plugin for Liferay on your Liferay server to index Liferay 6.1 content.

To deploy the Coveo Liferay portlet plugin

1. Using an administrator account, connect to the Coveo server.
2. From a browser, use an administrator account to connect to your Liferay portal.
3. On the menu bar of the Liferay portal, select Go to > Control Panel.
4. In the Liferay Control Panel:

   a. In the navigation panel on the left, under Server, click Plugins Installation.

   b. In the Plugins Installation page, select the Private Plugin Installer tab, and then go to step e)
Note: If you do not see the Private Plugin Installer tab:

i. Select the Portlet Plugins tab, and then click Install More Portlets.

ii. Follow the instructions starting at step c.

c. (When the Private Plugin Installer CE application is not installed on your Liferay portal) In the Liferay Marketplace:

i. In the Search box, enter private, press Enter, and then select Private Plugin Installer CE.

ii. In the Private Plugin Installer CE page, click Free.

iii. In the Purchase page:

A. Select an existing project or click Add a New Project.

B. When you click Add a New Project:

a. In the New Project dialog, enter a project name in the box, and then click Add.

b. Select the project you just created.

C. When you agree with the terms, select the I have read and agree to the End User License Agreement and the Terms of Service check box.

D. In the box at the bottom of the page, enter a Legal Entity Name.

E. Click Purchase.

F. On the Receipt page, select See Purchased.

G. In the Purchased Apps page, select the project in the Owner drop-down list, and then next to Private Plugin Installer CE, click Install.

iv. In the navigation panel on the left, under Server, click Plugins Installation.

d. In the Plugins Installation page, select the Private Plugin Installer tab.

e. In the Private Plugin Installer page:
i. Select the **Upload File** tab.

ii. **Click Choose File**, and then browse to and select the Coveo Liferay portlet plugin Web archive (WAR) file: `[CES_Path]\bin\CESLiferayConnector-portlet-6.0.6.1.war` or `[CES_Path]\bin\CESLiferayConnector-portlet-6.1.1.1.war`.

   **Example:** With the default installation path: `C:\Program Files\Coveo Enterprise Search 7\bin\CESLiferayConnector-portlet-6.0.6.1.war`

iii. **Click Install.**

f. End-users do not need to see the Coveo portlet. Consider hiding the Coveo portlet from users other than Administrator role members:

i. In the navigation panel on the left, under **Portal**, select **Plugins Configuration**.

ii. In the **Plugins Configuration** page, select the **CES Liferay Connector by Coveo Solutions Inc.** plugin.

iii. Under **Permissions**, for each user other than Administrator, click **Change**.

![Plugins Configuration](image)

iv. In the **Roles** page, clear the **Add to page** check box, and then click **Save**.

v. Navigate back to the **Plugins Configuration** page for the Coveo plugin, and then click **Save**.

5. You must also enable access to the Liferay Web services for the Coveo server:
a. Using an administrator account, connect to the Liferay server.

b. Using a text editor:
   i. Open, or create if it does not already exist, the [Liferay_Installation_Path]\tomcat-x.x.xx\webapps\ROOT\WEB-INF\classes\portal-ext.properties text file.

   ```
   axis.servlet.hosts.allowed=[Coveo_Server_IP_Address]
   axis.servlet.https.required=false
   tunnel.servlet.hosts.allowed=[Coveo_Server_IP_Address]
   tunnel.servlet.https.required=false
   ```

   where you replace [Coveo_Server_IP_Address] by the IP address of the Coveo Master server.

   iii. Restart the Liferay server to apply changes to the properties and activate the listeners used for incremental refresh by shutting down and restarting the Web server:

   **Example:** With a Tomcat server, in a command prompt window, run the following files:

   ```
   C:\Liferay6.1.1GA2\tomcat-7.0.27\bin\shutdown.bat
   C:\Liferay6.1.1GA2\tomcat-7.0.27\bin\startup.bat
   ```

   Restarting the server is required to apply changes to the properties and activate the listeners used for incremental refresh.

What's Next?

Create a Liferay account with which the Coveo connector can fully crawl the Liferay content (see "Setting up a Liferay Crawling Account" on page 1114).

9.23.7 Setting up a Liferay Crawling Account

The Coveo connector needs to connect to the Liferay portal using an account that has read access to all the Liferay content that you want to index. The Coveo connector only reads and does not modify the Liferay content.

The best practice is to create a Liferay fixed password account used exclusively by the Coveo connector and assigned to the built-in Administrator role that has complete access to all Liferay content.

**Setting up a dedicated Liferay full read account**

1. Using a Liferay account that has an Administrator role, sign in to your Liferay portal.

2. On the menu bar, select **Manage > Control Panel**.

3. In the Liferay **Control Panel**, in the navigation panel on the left under **Portal**, click **Users**.

4. In the **Users** page:
   a. Click **Add** to create a new user.
   b. Under **New User**, enter arbitrary information describing the Coveo Connector user.
   c. In the navigation menu on the right, click **Save**.
d. In the navigation menu on the right, under User Information, click Roles.

e. Under Regular Roles, click Select.

f. In the window that appears, under Roles, click the Administrator, to assign the Administrator role to the account.

g. If the Power User role has been assigned automatically, click Remove on the corresponding line, to ensure that only the Administrator role is assigned to this user.

h. In the navigation menu on the right, click Save.

i. In the navigation menu on the right, under User Information, click Password.

j. Enter a strong password in both the New Password and Enter Again boxes.

k. Leave the Password Reset Required checkbox cleared to prevent forcing the user to change the password when logging in the first time.

   Note: If the password changes in Liferay, you will also need to change it in the CES user identity (see "Adding a User Identity" on page 420).

l. In the navigation menu on the right, click Save.
What's Next?

On the Coveo server, configure a CES user identity for your Liferay crawling account (see "Adding a User Identity" on page 420).

Configure a security provider for your Liferay portal (see "Configuring a Liferay Security Provider" on page 1116).

9.23.8 CES Configuration for the Liferay Connector

9.23.8.1 Configuring a Liferay Security Provider

The Coveo connector needs a security provider to be able to get the permissions for each indexed Liferay item, and therefore fully support the Liferay security model. This means that, in a Coveo search interface, a user searching for Liferay content only sees the content to which he has access in the Liferay portal.

**Note:** You can get familiar with how Coveo components deal with permissions on documents both at indexing and query time.

To configure a Liferay security provider

1. On the Coveo server, access the Administration Tool.
3. In the Security page, in the navigation panel on the left, click Security Providers.
4. In the Security Providers page, click Add to create a new security provider.
5. In the Modify Security Provider page:
a. In the **Name** box, enter a name to identify this security provider.

   **Example**: Liferay Security Provider

b. In the **Security Provider Type** drop-down list, select **Liferay (x64)**.

c. In the **User Identity** section:
   
   i. In the drop-down list, select the user identity that you selected or created previously.
   
   ii. When needed, click **Add**, **Edit**, or **Manage user identities** respectively to create, modify, or manage user identities.

d. **CES 7.0.8047+ (December 2015)** (Optional) In the **Security Provider** section, in the drop-down list, select the security provider that you selected or created to allow this security provider to resolve and expand the groups (see **Liferay Connector Deployment Overview**).

e. In the **Liferay Portal Url** box, enter the address of the Liferay portal. This should be the same address as the one you will specify when you configure the source for the connector (see "Configuring and Indexing a Liferay Source" on page 1118). Enter the URL in the `http://[LiferayPortal]:[port]` form.

   **Example**: PortalUrl="http://MyLiferayPortal:8080"

f. When you have more than one company defined in your Liferay Portal, in the **Portal Web Id** box, enter
which company to index. Otherwise, leave this box empty.

**Note**: A company is associated with a WebId. You can find this ID in the Liferay Control Panel. Under Server, click Portal Instances, and then Web Id. There is a maximum of 1 ID per source. The default value is an empty string, which corresponds to the first WebId encountered.

g. In the Parameters section, in rare cases the Coveo Support could instruct you to click Add Parameters to specify other security provider parameter names and values that could help to troubleshoot security provider issues.

h. Leave the Allow Complex Identities option cleared as it does not apply to this type of security provider.

i. Click Save or Apply Changes, depending whether you are creating or modifying a security provider.

What's Next?

Configure and index a Liferay source (see "Configuring and Indexing a Liferay Source" on page 1118).

9.23.8.2 Configuring and Indexing a Liferay Source

A source defines a set of configuration parameters for a specific Liferay portal.

**Note**: In an environment with more than one Liferay portal, you need to define one source for each Liferay portal that you want to index.

To configure and index a Liferay source

1. On the Coveo server, access the Administration Tool.

2. Select Index > Sources and Collections.

3. In the Collections section:
   a. Select an existing collection in which you want to add the new source.

   OR

   b. Click Add to create a new collection.

4. In the Sources section, click Add.

   The Add Source page that appears is organized in three sections.

5. In the General Settings section of the Add Source page:
a. Enter the appropriate value for the following required parameters:

**Name**

Enter a descriptive name of your choice for the connector source.

**Example:** Liferay Portal

**Source Type**

Select the connector used by this source. In this case, select Liferay.

**Note:** If you do not see Liferay, your environment does not meet the requirements (see "Liferay Connector Requirements" on page 1107).

**Addresses**

Enter the root address of the Liferay portal in the format:

http://[servername]:[port]/

where you replace [servername]:[port] by the host name and port of your Liferay portal. The default port is 8080. The port is optional when equal to 80.

**Refresh Schedule**

Time interval at which the source is automatically refreshed to keep the index content up-to-date. The recommended **Every day** option instructs CES to refresh the source everyday at 12 AM.
Note: Incremental refresh does not catch changes to security and file attachment elements. Only a refresh does.

Note: You can create new or modify existing source refresh schedules.

b. Review the value for the following parameters that often do not need to be modified:

Rating

Change this value only when you want to globally change the rating associated with all items in this source relative to the rating to other sources.

Example: When a source replaces a legacy system, you may want to set this parameter to High, so that in the search interface, results from this source appear earlier in the list compared to those from legacy system sources.

Document Types

If you defined a custom document type set for this source, select it.

Active Languages

If you defined custom active language sets, ensure to select the most appropriate for this source.

Fields

If you defined custom field sets, ensure to select the most appropriate for this source.

6. In the Specific Connector Parameters & Options section of the Add Source page:
a. Review the value for the following parameters that often do not need to be modified:

**Mapping File**

Leave this field empty to use the default mapping file (see "About the Liferay Connector Mapping File" on page 1123). When you create a custom mapping file, enter the absolute full path pointing to your file (see "Customizing the Liferay Connector Mapping File" on page 1124).

**Example:** C:\CES7\Config\MyLiferayMappingFile.xml

**Index Blogs**

Whether blog entries, including their comments, should be indexed.

**Index Calendars**

Whether calendar events, including their comments, should be indexed.

**Index Document Libraries**

Whether document library files, including their comments, should be indexed.

**Index Message Boards**

Whether message board messages, including their attachments, should be indexed.

**Index Users**

Whether user profiles should be indexed.

**Index Web Content**

Whether web content, previously known as journals, should be indexed.

**Index Wikis**

Whether Wiki pages, including their attachments and comments, should be indexed.

**Authentication**

Select the user identity that you created previously for the Liferay portal.

**Parameters**

Click **Add Parameter** when you want to show advanced source parameters (see "Modifying Hidden Liferay Source Parameters" on page 1125).

**CES 7.0.8047+ (December 2015)** When you crawl a Liferay 6.1 instance, you must add the PluginUrl hidden parameter:

<table>
<thead>
<tr>
<th>Parameter name</th>
<th>Parameter value example</th>
</tr>
</thead>
<tbody>
<tr>
<td>PluginUrl</td>
<td>[LiferayServer:Port]/CESLiferayConnector-portlet/api/axis/Plugin_CES_LiferayConnectorService</td>
</tr>
</tbody>
</table>
In the **Option** section:

**Index Subfolders**

Keep this check box selected (recommended). By doing so, all subfolders from the specified portal address are indexed.

**Index the document's metadata**

When selected, CES indexes all the document metadata, even metadata that are not associated with a field. The orphan metadata are added to the body of the document so that they can be searched using free text queries.

When cleared (default), only the values of system and custom fields that have the **Free Text Queries** attribute selected will be searchable without using a field query.

**Example:** A document has two metadata:

- LastEditedBy containing the value Hector Smith
- Department containing the value RH

In CES, the custom field CorpDepartment is bound to the metadata Department and its **Free Text Queries** attribute is selected.

When the **Index the document's metadata** option is cleared, searching for RH returns the document because a field is indexing this value. Searching for hector does not return the document because no field is indexing this value.

When the **Index the document's metadata** option is selected, searching for hector also returns the document because CES indexed orphan metadata.

**Document's addresses are case-sensitive**

Leave the check box cleared. This parameter needs to be checked only in rare cases for systems in which distinct documents may have the same name but different casing.

**Generate a cached HTML version of indexed documents**

When you select this check box (recommended), at indexing time, CES creates HTML versions of indexed documents. In the search interfaces, users can then more rapidly review the content by clicking the Quick View link rather than opening the original document with the original application. Consider clearing this check box only when you do not want to use Quick View links or to save resources when building the source.

**Open results with cached version**

Leave this check box cleared (recommended) so that in the search interfaces, the main search result link opens the original document with the original application. Consider selecting this check box only when you do not want users to be able to open the original document but only see the HTML version of the document as a Quick View. In this case, you must also select **Generate a cached HTML version of indexed documents**.

7. In the **Security** section of the **Add Source** page:
a. In the **Security Provider** drop-down list, select the security provider that you created for this source (see "Configuring a Liferay Security Provider" on page 1116).

b. In the **Authentication** drop-down list, select the user identity that you created for the Liferay Portal.

c. Click **Save and Start** to save the source configuration and start indexing this source.

8. Validate that the source building process is executed without errors:

   - In the navigation panel on the left, click **Status**, and then validate that the indexing proceeds without errors.
   
   OR
   
   - Open the CES Console to monitor the source building activities.

What's Next?

Set an incremental refresh schedule for your source.

Add the built-in Liferay facet to your search interface (see "Managing Built-in Facets and Related Results Appearing in a .NET Search Interface" on page 574).

9.23.8.3 About the Liferay Connector Mapping File

The Liferay connector mapping file determines exactly which Liferay entities are indexed, what metadata is retrieved, and where this information is added in the Coveo unified index. The default mapping file ([CES_Path]\bin\Coveo.CES.CustomCrawlers.Liferay.DefaultMappingFile.xml) is automatically used when no mapping file is specified in the source.

The default mapping file specifies to index the following Liferay default entity types:

- Attachment
- BlogEntry
- CalendarEvent
- Comment
- DocumentLibraryFile
- MessageBoardMessage
User

WebContentLocalized

WikiPage

The mapping file is an XML file that contains various sections and subsections. The root element is `<LiferayMapping>`. It contains various `<Mapping>` nodes, each defining one entity type to be indexed with the corresponding metadata.

**Example:** The following mapping element specifies to index the BlogEntry entity type.

```xml
<Mapping type="BlogEntry">
  <Fields>
    <Title>%[title]</Title>
    <Body>%[content]</Body>
    <ClickableUri>%[coveo_url]</ClickableUri>
    <ModifiedDateUtc>%[coveo_lastModifiedDate]</ModifiedDateUtc>
    <CustomFields>
      <CustomField name="sysauthor">%[userName]</CustomField>
      <CustomField name="sysparents">%[coveo_breadcrumbs]</CustomField>
    </CustomFields>
  </Fields>
</Mapping>
```

A `<Mapping type="Default">` element applies to all retrieved items that do not have their own specific mapping element. Such an element exists but is commented out in the default mapping file.

**Note:** You can create and use a custom mapping file to fine-tune the Liferay indexed content (see "Customizing the Liferay Connector Mapping File" on page 1124).

### 9.23.8.4 Customizing the Liferay Connector Mapping File

The Coveo connector for Liferay portals comes with a default mapping file that makes the connector ready to index the default Liferay entities (see "About the Liferay Connector Mapping File" on page 1123).

You can customize the mapping file to fine-tune the indexed content or to include other Liferay entities.

To customize the mapping file

1. Using an administrator account, connect to the Coveo Master server.

2. Using a text editor:
   a. Open the default mapping file: `[CES_Path]\bin\Coveo.CES.CustomCrawlers.Liferay.DefaultMappingFile.xml`

   **Example:** With the default installation path: `C:\Program Files\Coveo Enterprise Search 7\Bin\Coveo.CES.CustomCrawlers.Liferay.DefaultMappingFile.xml`

   b. Save the file using a name of your choice in the `[Index_Path]\Config` folder.

   **Example:** With the default index path: `C:\CES7\Config\MyLiferayMappingFile.xml`

   c. Respecting the mapping file format (see "About the Liferay Connector Mapping File" on page 1123),
customize the file. Use the CustomFields section to directly reference columns present on a Liferay entity.

d. Save your changes.

What's Next?

Specify your customized mapping file in your Liferay source (see "Configuring and Indexing a Liferay Source" on page 1118).

9.23.8.5 Modifying Hidden Liferay Source Parameters

The Add Source and Source: ... General pages of the Administration Tool present the parameters with which you can configure the connector for most Liferay setups. More advanced and more rarely used parameters are hidden. You can choose to make one or more of these parameters appear in the Add Source and Source: ... General pages of the Administration Tool so that you can change their default value. Consider changing values of hidden parameters when you encounter issues.

The following list describes the advanced hidden parameters available with Liferay sources. The parameter type (integer, string,...) appears between parentheses following the parameter name.

PluginUrl (String) CES 7.0.8047+ (December 2015)

(For Liferay 6.1 only) The URL of the Coveo Liferay 6.1 plugin. The default value is null.

Example: [[LiferayServer:Port]]/CESLiferayConnector-portlet/api/axis/Plugin_CES_LiferayConnectorService

WebServiceBatchSize (Integer)

Number of items to fetch per request made to the Liferay portal. The default value is 300. The minimum value is 1. A small value forces the connector to make small but frequent queries to Liferay. A larger value leads to larger and less frequent queries.

CacheLifeSpan (Integer) OBSOLETE CES 7.0.8047– (December 2015)

The connector keeps a local cache of all the Liferay users. This way the connector doesn’t have to retrieve all users from Liferay on every full or Incremental refresh run. This parameter controls the amount of time (in minutes) this user cache will remain valid. When this delay expires, all users will be fetched again, instead of being taken out of the cache. The default value is 480 minutes (8 hours).

The amount of time (in minutes) the user cache that exists within the crawler lives. When this delay expires, all users will be fetched again, instead of being taken out of the cache. The default value is 480 minutes (8 hours).

BlogPortletId (String)
CalendarPortletId (String)
DocumentLibraryPortletId (String)
MessageBoardPortletId (String)
WikiPortletId (String)

These parameters tell the connector what is the ID of the portlet to use when creating clickable URLs for the different types of items. You must set these parameters only if your Liferay portal does not use the default
Example: BlogPortletId determines which portlet is used to present blogs. The default ID value is 33 for this portlet.

Note: You can find this information in the Liferay Control Panel. Under Portal, click Plugins Configuration. In the list of plugins that appears, click the desired plugin to see its information, including the Plugin ID (the information you must put in these parameters).

Languages (String)

The comma-separated list of languages to consider when retrieving Web Content. One item is returned per language. The parameter is empty by default and considers only the default portal language. Enter a * to specify all languages.

Example: en_US, fr_FR, de_DE, it_IT, ja_JP, es_ES

Note: You can find possible languages in the Liferay Control Panel. Under Portal, click Plugins Configuration. In the list of plugins that appears, click the desired plugin to see its information, including the Plugin ID (the information you must put in these parameters).

SiteMinderFormLoginAction (String)

This parameter, along with the SiteMinderFormLoginPage parameter, is only required when Liferay resides inside a SiteMinder secure realm. These parameters enable the connector to authenticate with SiteMinder in order to gain access to the Liferay server so it can retrieve the content to index. This parameter contains the POST action that will be sent to the SiteMinder authentication form (login.fcc).

Example: USER=username&PASSWORD=password&SMAUTHREASON=0&TARGET=https%3a%2f%2fliferayportal

Note: The POST action contains four parameters: USER, PASSWORD, SMAUTHREASON, and TARGET. USER and PASSWORD are the credentials to authenticate to SiteMinder. SMAUTHREASON is always equal to zero. The TARGET parameter is the secure resource you want to access, in this case the Liferay portal URL (https://liferayportal), and must be properly escaped.

SiteMinderFormLoginPage (String)

This parameter is the URL of the SiteMinder authentication form (login.fcc).

Example: https://www.acme.com/siteminderagent/forms/login.fcc

Note: Ask your SiteMinder administrator for the URL of the authentication form.

NumberOfRefreshThreads (Integer)

This determines the number of threads that simultaneously crawl the Liferay portal. The default value is 2.

WebId (String)

This parameter determines which company to index. A company is associated with a WebId.
Note: You can find this ID in the Liferay Control Panel. Under Server, click Portal Instances, and then Web Id. There is a maximum of 1 ID per source. The default value is an empty string, which corresponds to the first WebId encountered.

Use the following procedure only when you want to modify one or more of the above hidden source parameters.

To modify hidden Liferay source parameters

1. Refer to "Adding an Explicit Connector Parameter" on page 450 to add one or more Liferay hidden source parameters.

2. For a new Liferay source, access the Add Source page of the Administration Tool to modify the value of the newly added advanced parameter:
   a. Select Index > Sources and Collections.
   b. Under Collections, select the collection in which you want to add the source.
   c. Under Sources, click Add.
   d. In the Add Source page, edit the newly added advanced parameter value.

3. For an existing Liferay source, access the Source: ... General page of the Administration Tool to modify the value of the newly added advanced parameter:
   a. Select Index > Sources and Collections.
   b. Under Collections, select the collection containing the source you want to modify.
   c. Under Sources, click the existing Liferay source in which you want to modify the newly added advanced parameter.
   d. In the Source: ... General page, edit the newly added advanced parameter value.

4. Rebuild your Liferay source to apply the changes to the parameters.

9.24 Lithium Connector

CES 7.0.6767+ (June 2014)

Lithium is a social customer experience management software for the enterprise. The Coveo connector for Lithium communities allows you to crawl and bring Lithium content into the unified index, making it easily searchable by end-users.

9.24.1 Connector Features Summary

<table>
<thead>
<tr>
<th>Features</th>
<th>Supported</th>
<th>Additional information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Lithium version</td>
<td>Latest cloud version</td>
<td>Following available Lithium releases</td>
</tr>
<tr>
<td>Features</td>
<td>Supported</td>
<td>Additional information</td>
</tr>
<tr>
<td>------------------</td>
<td>-----------</td>
<td>----------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Searchable content types</td>
<td>✔️</td>
<td>Community, categories, boards, and discussions (also known as threads and conversations) including topics (texts and products), replies (answers, comments, and reviews), and messages (replies) also known as posts.</td>
</tr>
<tr>
<td>Content refresh</td>
<td></td>
<td><strong>Incremental refresh</strong> ✔️ CES 7.0.9093+ (September 2017) Incremental refresh support. A full refresh or rebuild is required to take account of modified and deleted items.</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Full refresh</strong> ✔️</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Rebuild</strong> ✔️</td>
</tr>
<tr>
<td>Document-level security</td>
<td>✗</td>
<td>Permissions must be manually defined on the source [more]</td>
</tr>
</tbody>
</table>

### 9.24.2 Features

The features of the Lithium connector are:

#### Content indexing

The connector can retrieve and index exclusively the following Lithium content type shown hierarchically:

- Community
  - Categories
    - Boards
      - Discussions (aka threads, conversations)
        - Topics
          - Text
          - Products
        - Replies
          - Answers
          - Comments
          - Reviews
      - Messages (aka posts)
        - Replies
Partial Incremental Refresh

The connector supports incremental refresh allowing to maintain the source up-to-date with your Lithium community by indexing at regular short intervals new Lithium community items.

**Note:** Changed and deleted items require a source full refresh or rebuild to be taken into account.

**Important:** The Lithium connector cannot index Lithium permissions because the Lithium API does not allow user permission retrieval for each item. This means that any user having access to Coveo search results from a Lithium source can find any Lithium item indexed by the crawling account, regardless of whether they are allowed to access these items in Lithium.

Feature history

<table>
<thead>
<tr>
<th>CES version</th>
<th>Monthly release</th>
<th>Features</th>
</tr>
</thead>
<tbody>
<tr>
<td>7.0.9093+</td>
<td>September 2017</td>
<td>Incremental refresh support</td>
</tr>
<tr>
<td>7.0.6767+</td>
<td>June 2014</td>
<td>Connector introduction in general availability (GA).</td>
</tr>
</tbody>
</table>

9.24.3 Lithium Connector Deployment Overview

The following procedure outlines the steps needed to deploy the Lithium connector. The steps indicate the order in which you must perform configuration tasks in both Lithium and Coveo.

1. Validate that your environment meets the requirements:
   - CES 7.0.6767+ (June 2014)
     - Lithium connector included in your Coveo license
     - A Lithium account having access to all the Lithium content that you wish to index

2. When you want to index secured Lithium content, in Lithium, select or create the crawling account.
   - The Coveo connector needs a Lithium account such as an administrator account with which it can fully crawl the Lithium content. Moreover, this account must have permission to make REST API read calls. This setting is available in your Lithium Community admin section, under **Users > Permissions > Make REST API calls with read access**.

3. In the Coveo Administration Tool:
   a. When you want to index secured Lithium content, configure a user identity.
      - The Coveo connector needs to know the Lithium account that you previously selected or created. You must create a CES user identity to use this account.
b. Optionally, create a Lithium field set from the default XML field set file to be able to leverage Lithium metadata for example to create more useful facets.

Copy the content of the default XML Lithium field set file (C:\Program Files\Coveo Enterprise Search 7\Bin\Coveo.CES.CustomCrawlers.Lithium.FieldSet.xml), and then import it to create a Lithium field set.

c. Configure and index the Lithium source.

The Coveo connector needs to know details about the Lithium community to be able to index its content (see "Configuring and Indexing a Lithium Source" on page 1130).

What's Next?

In the Interface Editor, create or modify a search interface to include facets based on Lithium fields to allow user to more easily drill-down in Lithium content.

9.24.4 Configuring and Indexing a Lithium Source

A source defines a set of configuration parameters for a specific Lithium community. When you want to index more than one Lithium community, configure one source for each community.

To configure and index a source with the Lithium connector

1. On the Coveo server, access the Administration Tool.

2. Select Index > Sources and Collections.

3. In the Collections section:

   a. Select an existing collection in which you want to add the new source.

       OR

   b. Click Add to create a new collection.

4. In the Sources section, click Add.

5. In the General Settings section of the Add Source page:
a. Enter the appropriate value for the following required parameters:

**Name**

Enter a descriptive name of your choice for the connector source.

**Example:** Lithium Community

**Source Type**

The connector used by this source. In this case, select Lithium.

**Addresses**

Enter the URL of the Lithium community to index. Enter only one Lithium community address. Create other sources for other communities.

**Examples:** The Lithium community addresses can be:

- http://companynname.lithium.com/
- https://community.companynname.com/
Notes:

- You can also specify to crawl only a subset of a Lithium community by simply copying and pasting the address of a Lithium category, board, or thread. The URL is in the form:

  http://community.company.com/[...]/lithiumobjectlabel/objectid

  where the possible values for lithiumobjectlabel are given in the Label column in the following table.

<table>
<thead>
<tr>
<th>Label</th>
<th>Lithium object</th>
</tr>
</thead>
<tbody>
<tr>
<td>ct-p</td>
<td>Category</td>
</tr>
<tr>
<td>tkbc-p</td>
<td>Knowledge base category</td>
</tr>
<tr>
<td>bd-p</td>
<td>Forum</td>
</tr>
<tr>
<td>tkb-p</td>
<td>Knowledge base</td>
</tr>
<tr>
<td>con-p</td>
<td>Contest</td>
</tr>
<tr>
<td>idb-p</td>
<td>Idea board</td>
</tr>
<tr>
<td>qa-p</td>
<td>Q&amp;A board</td>
</tr>
<tr>
<td>bg-p</td>
<td>Blog</td>
</tr>
<tr>
<td>gp-p</td>
<td>Group</td>
</tr>
<tr>
<td>m-p</td>
<td>CES 7.0.7599+ (April 2015) Forum thread</td>
</tr>
<tr>
<td>td-p</td>
<td>Forum thread</td>
</tr>
<tr>
<td>ta-p</td>
<td>Knowledge base article</td>
</tr>
<tr>
<td>cns-p</td>
<td>Contest submission</td>
</tr>
<tr>
<td>idi-p</td>
<td>Idea</td>
</tr>
<tr>
<td>qaq-p</td>
<td>Q&amp;A Question</td>
</tr>
<tr>
<td>ba-p</td>
<td>Blog article</td>
</tr>
<tr>
<td>gpm-p</td>
<td>Group article</td>
</tr>
</tbody>
</table>

Example: On the Lenovo Lithium community the following address is for the CES2014 forum:


- If you use a reverse proxy, your REST API might not reside at your community root URL. You
must therefore add the `RestApiUrl` hidden parameter to specify the URL address at which your REST API resides (see "Modifying Hidden Lithium Source Parameters" on page 1138). Be aware, however, that Lithium does not recommend using a reverse proxy (see Reverse proxy and Lithium communities while logged in with a Lithium account).

### Fields

If you created a custom Lithium field set, select it (see Lithium Connector Deployment Overview). Otherwise, leave the Default Scheme.

### Refresh Schedule

Select the time interval at which the source is automatically refreshed to keep the index content up-to-date. By default, the Every day option instructs CES to refresh the source everyday at 12 AM. Because the incremental refresh takes care of maintaining the source up-to-date, you can select a longer interval such as Every Sunday.

### Notes:

- You must enable incremental refresh on your source to continuously maintain the index up-to-date with your source between full refreshes.

  - **CES 7.0.8996– (June 2017)** The Lithium connector does not support incremental refresh. Consequently, the full refresh schedule is the only process that keeps your source up-to-date.

b. Review the value for the following parameters that often do not need to be modified:

### Rating

Change this value only when you want to globally change the rating associated with all items in this source relative to the rating to other sources.

**Example:** If this source was for a legacy Lithium community, you may want to set this parameter to Low, so that in the search interface, results from this source appear later in the list compared to those from other sources.

### Document Types

If you defined custom document type sets, ensure to select the most appropriate for this source.

### Active Languages

If you defined custom language sets, ensure to select the most appropriate for this source.

6. In the Specific Connector Parameters & Options section of the Add Source page:
a. Review if you need to change the default values for the following parameters:

**Number of Refresh Threads**

Determine the number of simultaneous downloads handled by the connector for this source. The default value is 2.

**Mapping File**

The path to the mapping file. Leave the default value to use the default mapping file that comes with the connector (Coveo.CES.CustomCrawlers.Lithium.MappingFile.xml). If you create a custom mapping file, enter the full path to your custom mapping file. Contact Coveo Support for assistance if you need to customize the mapping file.

b. **CES 7.0.9093+ (September 2017)** Select the following checkboxes if you want to index the corresponding content:

- **Index attachments**
  Select this option to index message attachments, such as images, videos, and PDF files.

  **Notes:**
  
  - For attachments to be indexed, the hidden parameter `ItemTypesToIndex` value must be empty or contain `attachment` as well (see Modifying Hidden Lithium Source Parameters).
  - Selecting this option requires one more API call per message.
  - **CES 7.0.8996+ (June 2017)** For attachments to be indexed as well, you must add the `FetchMessageAttachments` hidden parameter (see FetchMessageAttachments and "To modify hidden Lithium source parameters" on page 1140).

- **Index users**
  Select this option to index data regarding users of a community.
For users to be indexed, the hidden parameter ItemTypesToIndex value must be empty or contain user as well (see Modifying Hidden Lithium Source Parameters).

You can index users only when indexing an entire community. If you only index a community subset such as a category or a board, you cannot index users (see Note: Crawling a community subset).

Indexing users of a large Lithium community can have a significant impact on the indexing process performance.

For users to be indexed as well, you must add the FetchUsers hidden parameter (see FetchUsers and "To modify hidden Lithium source parameters" on page 1140).

c. In the Parameters section, click Add Parameter to be able to change the default value of hidden parameters (see "Modifying Hidden Lithium Source Parameters" on page 1138).

<table>
<thead>
<tr>
<th>Hidden parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>AuthenticationFormId</td>
<td>if not the default (form)</td>
</tr>
<tr>
<td>LoginPageUrl</td>
<td>The login page URL</td>
</tr>
<tr>
<td>LoginFieldName</td>
<td>if not the default (login)</td>
</tr>
<tr>
<td>PasswordFieldName</td>
<td>if not the default (password)</td>
</tr>
<tr>
<td>UseFormAuthenticationToFetchAttachments</td>
<td>true</td>
</tr>
</tbody>
</table>

Note: When you want to index the content of a Lithium community that is secured using form authentication, add the following hidden parameters (see "Modifying Hidden Lithium Source Parameters" on page 1138).

d. In the Option section, review the default value of the following check boxes:

Index Subfolders

Check to index all subfolders below the specified Lithium server address. Selected by default.

Index the document’s metadata

When selected, CES indexes all the document metadata, even metadata that are not associated with a field. The orphan metadata are added to the body of the document so that they can be searched using free text queries.

When cleared (default), only the values of system and custom fields that have the Free Text Queries attribute selected will be searchable without using a field query.
Example: A document has two metadata:

- LastEditedBy containing the value Hector Smith
- Department containing the value RH

In CES, the custom field CorpDepartment is bound to the metadata Department and its Free Text Queries attribute is selected.

When the Index the document's metadata option is cleared, searching for RH returns the document because a field is indexing this value. Searching for hector does not return the document because no field is indexing this value.

When the Index the document's metadata option is selected, searching for hector also returns the document because CES indexed orphan metadata.

Generate a cached HTML version of indexed documents

When you select this check box (recommended), at indexing time, CES creates HTML versions of indexed documents. In the search interfaces, users can then more rapidly review the content by clicking the Quick View link rather than opening the original document with the original application. Consider clearing this check box only if you do not want to use Quick View links or to save resources when building the source.

Open results with cached version

Leave this check box cleared (recommended) so that in the search interfaces, the main search result link opens the original document with the original application. Consider selecting this check box only when you do not want users to be able to open the original document but only see the HTML version of the document as a Quick View. In this case, you must also select Generate a cached HTML version of indexed documents.

7. In the Security section of the Add Source page:

- In the Authentication drop-down list:
  - When you want to index secured Lithium content, select the user identity that you created for the Lithium community to index.

  Note: The user identity you select must be a native Lithium user. An SSO user cannot be used to retrieve secured Lithium content.
OR

- When you index a public Lithium community, select (none).

b. Click Save to save the source configuration.

8. Because the Lithium connector does not support indexing Lithium item permissions, you must rather set the permissions globally on the source:

**Note:** You get the following error message in the CES Console when you try to index the permissions for a Lithium community source.

Error with ID 'LITHIUM_INVALID_CONFIGURATION': Permissions indexing is not provided by the Lithium connector

a. In the navigation panel on the left, select Permissions.

b. In the Permissions page:

i. Select the **Specifies the security permissions to index** option.

ii. Optionally, in the Allowed Users list, add or remove users or groups to precisely specify who has access to the content from this source. By default, the Active Directory **everyone** group specifies that any AD user can see all the content from this source.
iii. Optionally, in the **Denied Users** list, add users or groups to specify who has not access to the content from this source.

iv. Click **Apply Changes**.

9. On the toolbar, click **Start/Rebuild** to start indexing your source.

10. Validate that the source building process is executed without errors:

    - In the navigation panel on the left, click **Status**, and then validate that the indexing proceeds without errors.
    
    OR
    
    - Open the CES Console to monitor the source building activities.

What's Next?

Consider modifying some hidden source parameters to try resolving other issues (see "Modifying Hidden Lithium Source Parameters" on page 1138).

- CES 7.0.9034+ (September 2017) Set an incremental refresh schedule for your source.

9.24.5 Modifying Hidden Lithium Source Parameters

The **Add Source** and **Source: ... General** pages of the Administration Tool present the parameters with which you can configure the connector for most Lithium setups. More advanced and more rarely used parameters are hidden. You can choose to make one or more of these parameters appear in the **Add Source** and **Source: ... General** pages of the Administration Tool so that you can change their default value. Consider changing values of hidden parameters when you encounter issues.

The following list describes the advanced hidden parameters available with Lithium sources. The parameter type (integer, string…) appears between parentheses following the parameter name.

**RestApiUrl** CES 7.0.9434+ (September 2018)

If you use a reverse proxy, your REST API might not reside at your community root URL. You must therefore add the **RestApiUrl** hidden parameter to specify the URL address at which your REST API resides.

*Note:* Lithium does not recommend using a reverse proxy (see Reverse proxy and Lithium communities while logged in with a Lithium account).

**BasicAuthenticationUsername** (String)**

**BasicAuthenticationPassword** (String)

The user name and password to use when the Lithium community is secured with basic (http) authentication.

**FetchMessageTags** (Boolean)

Indicates whether to fetch the tags associated with the messages. The default is true.

**FetchMessageAttachments** (Boolean) CES 7.0.8996+ (June 2017)

Indicates whether to fetch the attachments associated with the messages. The default is true.
**Note:** Setting this parameter to `true` requires one more API call per message.

**FetchUsers (Boolean) [CES 7.0.8996–(June 2017)]**

Indicates whether to fetch users. The default is `false`.

**Notes:**
- You can index users only when indexing an entire community. If you only index a community subset such as a category or a board, you cannot index users.
- On a large Lithium community, indexing the users may take a significant amount of time.

**ApiVersion (String) [CES 7.0.8996–(June 2017)]**

The version of the Lithium REST API to use: `vx`, `vc`, or `v1`. The default is `v1`.

**LoginPageUrl (String)**

The login page URL to use when the community uses form authentication. You can get this URL by attempting to access the Lithium community while you are not yet logged in.

**Example:** `https://community.lithium.com/t5/user/userloginpage`

**LoginFieldName (String)**

The name of the form authentication login field. The default is `login`. Inspect the login page to find the `<input... name="login" ...>` tag for the user name field and copy the value of its `name` attribute to put in this parameter.

**PasswordFieldName (String)**

The name of the form authentication password field. The default is `password`. Inspect the login page to find the `<input... name="password" ...>` tag for the password field and copy the value of its `name` attribute to put in this parameter.

**AuthenticationFormId (String)**

The form authentication ID to use. The default is `form`. Inspect the login page to find the `<form ... id="form" name="form">` tag and copy the value of its `id` attribute to put in this parameter.

**AdditionalFormParameters (String)**

When needed, a list of additional form authentication parameters formatted as follows:

'param1=value1;param2=value2'

**UseFormAuthenticationToFetchAttachments (Boolean)**

Whether to use form authentication to fetch attachments. The default is `false`.

**IndexMessageHasEmbeddedImage (Boolean) [CES 7.09093+ (September 2017)]**

Whether to set a metadata value indicating that the message has at least one embedded image. The default is `false`.
IndexMessageHasEmbeddedVideo (Boolean) CES 7.0.9093+ (September 2017)
Whether to set a metadata value indicating that the message has at least one embedded video. The default is false.

ItemTypesToIndex (String) CES 7.0.9093+ (September 2017)
The item types to index. The default is empty, which indexes all item types (see "Searchable content types" on page 1128). You can select specific item types to index by entering the desired types separated by semicolons.
Example: community;category;board;thread:message;attachment;user

NumberOfRetries (Integer) CES 7.0.9093+ (September 2017)
The number of retries allowed when a web request fails. The default is 3.

PageSize (Integer) CES 7.0.9093+ (September 2017)
The number of items returned for an API call. The default is 50, the upper limit is 100.

Use the following procedure only when you want to modify one or more of the above hidden source parameters.

To modify hidden Lithium source parameters

1. Refer to "Adding an Explicit Connector Parameter" on page 450 to add one or more Lithium hidden source parameters.

2. For a new Lithium source, access the Add Source page of the Administration Tool to modify the value of the newly added advanced parameter:
   a. Select Index > Sources and Collections.
   b. Under Collections, select the collection in which you want to add the source.
   c. Under Sources, click Add.
   d. In the Add Source page, edit the newly added advanced parameter value.

3. For an existing Lithium source, access the Source: ... General page of the Administration Tool to modify the value of the newly added advanced parameter:
   a. Select Index > Sources and Collections.
   b. Under Collections, select the collection containing the source you want to modify.
c. Under Sources, click the existing Lithium source in which you want to modify the newly added advanced parameter.

d. In the Source: ... General page, edit the newly added advanced parameter value.

4. Rebuild your Lithium source to apply the changes to the parameters.

9.25 Microsoft Active Directory Connector

You can use the Microsoft Active Directory connector to index user information stored in Active Directory. The connector uses incremental refresh to periodically query Active Directory for the latest content modifications and keep the index up-to-date.

Deployment overview

1. Create a user identity for your Active Directory source

   The Active Directory content is accessible in read-only to any user from the domain or from a trusted domain. The Active Directory connector can therefore use any Active Directory user to crawl and index the Active Directory content. You must configure a CES user identity that contains information about the user you choose to use (see "Adding a User Identity" on page 420). You will later assign this user identity to your Active Directory source and security provider.

   **Note:** A best practice is to create an Active Directory user dedicated to the CES connector and for which the password never changes.

2. (Optional) Modify the default Active Directory security provider or create a new one

   Coveo Enterprise Search (CES) comes with a default Active Directory security provider. You can modify this security provider or create new ones to connect to a specific Active Directory domain (see "Configuring an Active Directory Security Provider" on page 1141).

   **Example:** In your organization, there are several Microsoft Windows domains. You want to index the Active Directory content of Domain A while CES is running in DomainC. You can create a Domain A security provider and assign it to a Domain A Active Directory source to index only the Active Directory content of this domain.

3. Configure and index a Microsoft Active Directory source (see "Configuring and Indexing an Active Directory Source" on page 1143).

9.25.1 Configuring an Active Directory Security Provider

You must use an Active Directory (AD) security provider when you create a source to index the content of an Active Directory domain. Other security providers may need to use an Active Directory security provider to expand, map, or resolve users or groups defined in Active Directory.

Coveo Enterprise Search (CES) comes with a default Active Directory security provider to which no user identity is assigned. In this case, the Active Directory security provider takes the CES service account as the user to access AD. When CES is in the same domain as AD, you can use the default Active Directory security provider as is. No configuration is needed.
You may need to create another Active Directory security provider only when CES and AD are in different and untrusted domains. In this case, you only need to assign a user identity containing any user that has access to the other domain to be able to use the security provider to expand, map, or resolve users or groups defined in Active Directory of this domain.

Note: You can get familiar with how Coveo components deal with permissions on documents both at indexing and query time.

To create or modify an Active Directory security provider

1. On the Coveo server, access the Administration Tool.
3. In the navigation panel on the left, select Security Providers.
4. In the Security Providers page:
   - Click Add to create a new security provider.
   - OR
   - Click an existing Active Directory security provider to modify it.
5. In the Modify Security Provider page:
a. In the **Name** box, enter a name to identify this security provider.

b. In the **Security Provider Type** drop-down list:
   i. On a 32-bit server, select **Active Directory (x86)**.
   ii. On a 64-bit server, select **Active Directory (x64)**.

c. In the **User Identity** section:
   i. In the drop-down list, select a user identity containing an account that has access to the desired domain.

```
Example: When the user identity contains the domainA\OneUsername account, the security provider connects to Domain A Active Directory.
```

**Note:** When **User Identity** is set to **(none)**, the security provider takes the CES service account by default.

ii. When needed, click **Add**, **Edit**, or **Manage user identities** respectively to create, modify, or manage user identities.

d. **CES 7.0.7338+ (January 2015)** In the **Email Provider** section:
   i. In the drop-down list, select the email provider that recognizes your users by their email addresses.

```
Note: When you do not want to map Active Directory (AD) users to their email, select **(none)**.
```

ii. When needed, click **Add**, **Edit**, or **Manage security providers** respectively to create, modify, or manage email security providers.

e. In the **Parameters** section, in rare cases the Coveo Support could instruct you to click **Add Parameters** to specify other security provider parameter names and values that could help to troubleshoot security provider issues.

f. Leave the **Allow Complex Identities** option cleared as it does not apply to this type of security provider.

g. Click **Save** or **Apply Changes**, depending whether you are creating or modifying a security provider.

**What's Next?**

When you are creating or modifying the security provider:

- For an Active Directory source, configure and index the source.
- To be used by another security provider, create or modify the other security provider.

**9.25.2 Configuring and Indexing an Active Directory Source**

A source defines a set of connector parameters specifying where and how to crawl Active Directory in a given domain. The Coveo connector for Microsoft Active Directory uses the Lightweight Directory Access Protocol (LDAP) to read Active Directory content. The connector performs an LDAP search to find all the items to index.
To configure and index an Active Directory source

1. On the Coveo server, access the Administration Tool.
2. Select Index > Sources and Collections.
3. In the Collections section:
   a. Select an existing collection in which you want to add the new source.
   OR
   b. Click Add to create a new collection.
4. In the Sources section, click Add.
5. In the General Settings section of the Add Source page:

   a. Enter the appropriate value for the following required parameters:

   Name
     Enter a descriptive name of your choice for the connector source.

   Example: Active Directory Domain A

   Source Type
     Select the connector used by this source. In this case, select Active Directory.
Addresses

The list of LDAP URIs indicating the starting locations to index, one entry per line.

**Example:** With the `domainA.MyOrganization.com` domain, acceptable values can be:
- LDAP://MyOrganization
- LDAP://domainA.MyOrganization.com
- LDAP://DC=domainA,DC=MyOrganization,DC=com

If you want to select only users from a particular organization unit (OU), enter the address in the form:
- LDAP://OU=ouName,DC=domainA,DC=MyOrganization,DC=com

**Important:** In the LDAP URLs, you must enter the keywords (LDAP, OU, DC...) in uppercase.

b. Review the value for the following parameters that often do not need to be modified:

**Rating**

Change this value only when you want to globally change the rating associated with all items in this source relative to the rating of elements in other sources.

**Document Types**

If you created a custom document type set for this source, select it.

**Active Languages**

If you defined custom active language sets, ensure to select the most appropriate for this source.

**Fields**

If you defined custom field sets, ensure to select the most appropriate for this source.

**Refresh Schedule**

Time interval at which the index is automatically refreshed to keep the index content up-to-date. By default, the recommended **Every day** option instructs CES to refresh the source everyday at 12 AM.

**Note:** You can create new or modify existing source refresh schedules.

6. In the **Specific Connector Parameters & Options** section of the **Add Source** page:
a. Enter the appropriate value for the following parameters:

**Incremental Refresh Delay**

Determines the time interval in seconds between incremental refresh updates. The default and recommended value is 3600 seconds (1 hour).

**LDAP Filters**

The filters used to refine the LDAP query to Active Directory. You typically want to crawl all the users in Active Directory. Depending on the configuration of Active Directory, you may find that unwanted users are crawled. The default value is mail=*.

It allows to get all users that also have an Exchange Mailbox.

**Note:** The connector includes a built-in hidden filter: \( (&(objectclass=user)\) (objectclass=person))\). This is a logical AND operation that finds users that are real persons, eliminating other mailboxes. The filter you enter in **LDAP Filters** is added to the AND operation of the built-in hidden filter (ex.: \( (&(objectclass=user)\) (objectclass=person) \) mail=*)\).

**Parameters**

Click **Add Parameter** when you want to show advanced hidden source parameters.

b. In the **Option** section, review the value for the following parameters that often do not need to be modified:

**Index Subfolders**

Check to index all subfolders below the specified starting addresses. Selected by default.

**Index the document's metadata**

When selected, CES indexes all the document metadata, even metadata that are not associated with a field. The orphan metadata are added to the body of the document so that they can be searched using free text queries.

When cleared (default), only the values of system and custom fields that have the **Free Text Queries** attribute selected will be searchable without using a field query.
Example: A document has two metadata:

- LastEditedBy containing the value Hector Smith
- Department containing the value RH

In CES, the custom field CorpDepartment is bound to the metadata Department and its Free Text Queries attribute is selected.

When the Index the document's metadata option is cleared, searching for RH returns the document because a field is indexing this value. Searching for hector does not return the document because no field is indexing this value.

When the Index the document's metadata option is selected, searching for hector also returns the document because CES indexed orphan metadata.

Document's addresses are case-sensitive

Leave the check box cleared. This parameter needs to be checked only in rare cases for case sensitive systems in which distinct documents may have the same file name but with different casing.

Generate a cached HTML version of indexed documents

When you select this check box (recommended), at indexing time CES creates HTML versions of indexed documents and saves them in the unified index. In the search interfaces, users can then more rapidly review the content by clicking the Quick View link to open the HTML version of the item rather than opening the original document with the original application.

Consider clearing this check box only if you do not want to use Quick View links or to save resources when building the source.

Open results with cached version

Leave this check box cleared (recommended) so that in the search interfaces, the main search result link opens the original document with the original application. Consider selecting this check box only when you do not want users to be able to open the original document but only see the HTML version of the document as a Quick View. When this option is selected, you must also select the Generate a cached HTML version of indexed documents check box.

7. In the Security section of the Add Source page:
In the **Security Provider** drop-down list, select the default, modified, or new Active Directory security provider that want for this source (see "Configuring an Active Directory Security Provider" on page 1141).

b. In the **Authentication** drop-down list, select the user identity that you selected for this source (see "Adding a User Identity" on page 420).

c. Click **Save and Start** to save the source configuration and start indexing this source.

8. Validate that the source building process is executed without errors:
   - In the navigation panel on the left, click **Status**, and then validate that the indexing proceeds without errors.
     - OR
   - Open the CES Console to monitor the source building activities.

What's Next?

Set an incremental refresh schedule for your source.

Add the collection containing this new source to the scope of desired search interfaces.

9.26 Microsoft Dynamics CRM Connector

**CES 7.0.7338+ (January 2015)**

This Coveo connector for Microsoft Dynamics CRM systems allows users to search Microsoft Dynamics CRM entities. Microsoft Dynamics CRM is a system that provides a set of customer relationship management (CRM) functions.

**Notes:**

- The document in this section describes the second generation Dynamics connector.
- **CES 7.0.7599+ (April 2015)** The connector supports the 2013 and 2015 versions of Microsoft Dynamics CRM On-Premises, and Microsoft Dynamics CRM Online.
- For users of the Microsoft Dynamics CRM legacy connector, it is recommended to upgrade to this version. Contact Coveo Support if you need assistance.

The features of the Microsoft Dynamics CRM connector are:

**Content Indexing**

- Retrieval and indexing of the following Dynamics object types:
  - All available Microsoft Dynamics CRM system entities and custom ones
  - Notes and files attached to records of the indexed entity types
  - **CES 7.0.7711+ (June 2015)** KB Articles (body, comments, attachments)

**Fully Supported Security Model** **CES 7.0.7599+ (April 2015)**

The connector fully supports the Microsoft Dynamics CRM security model (role-based and object-based...
permissions). This means that, in the Coveo search interface, a user searching Microsoft Dynamics CRM content only sees the content to which he has access in the Microsoft Dynamics CRM system.

The security features supported are:

- Users
- Security Roles (privileges)
- Business Unit
- Teams
- Hierarchical permissions
- Sharing

**Pause/Resume**

When indexing Microsoft Dynamics CRM systems, the connector can be paused and resumed.

**Incremental Refresh**

Periodically queries Microsoft Dynamics CRM systems for the latest items modifications (addition, edition, deletion), keeping the index content up-to-date.

**Notes:**

- Auditing must be enabled for indexed entities for the connector to be able to retrieve deleted items (see "Enabling Auditing of Your Microsoft Dynamics CRM Entities" on page 1152).
- **CES 7.0.7433+ (February 2015)** The incremental refresh supports deleted items.
- **CES 7.0.7711+ (June 2015)** The incremental refresh supports out-of-the-box attachments modifications (addition, edition).
- Some events in Microsoft Dynamics CRM require a source refresh or a security cache update to be retrieved by the connector and applied to the source (see "Microsoft Dynamics CRM Events Update Requirements" on page 1153).

**9.26.1 Limitations**

- Fields security profiles are not yet supported.
- **CES 7.0.7599– (April 2015)** The connector does not support Dynamics CRM security model (role-based and object-based permissions).

**Important:** In the Coveo search interface, a user searching Dynamics CRM 2013 On-Premises and Online content could see content to which he has normally no access in the Dynamics CRM system. Thus, it is highly recommended to only index Dynamics system(s) with public content.
Feature History

<table>
<thead>
<tr>
<th>CES version</th>
<th>Monthly release</th>
<th>Features</th>
</tr>
</thead>
<tbody>
<tr>
<td>7.0.7711</td>
<td>June 2015</td>
<td>Incremental refresh supports out-of-the-box attachment modifications (addition, edition)</td>
</tr>
</tbody>
</table>
| 7.0.7599    | April 2015      | - Support of Dynamics CRM 2015 On-Premises  
|             |                 |   - Full support of security model  
|             |                 |   - Support entity relationships |
| 7.0.7433    | February 2015   | Incremental refresh supports deleted items |
| 7.0.7338    | January 2015    | Connector introduction |

What's Next?

Review the deployment process (see "Microsoft Dynamics CRM Connector Deployment Overview" on page 1150).

9.26.2 Microsoft Dynamics CRM Connector Deployment Overview

The following procedure outlines the steps needed to deploy the second generation Microsoft Dynamics CRM connector. The steps indicate the order in which you must perform configuration tasks on both the CES and Microsoft Dynamics CRM systems.

1. Validate that your environment meets the requirements (see "Microsoft Dynamics CRM Connector Requirements" on page 1151).

2. In the Microsoft Dynamics CRM system:
   a. Select or create the crawling account.

   The CES connector needs a Microsoft Dynamics CRM account with which it can crawl the Microsoft Dynamics CRM content (see "Setting Up a Microsoft Dynamics CRM Full Read Account" on page 1155).

   b. (Optionally) Enable the auditing on all entities you want to index

   The auditing must be enabled on entities for the connector to be able to retrieve deleted items (see "Enabling Auditing of Your Microsoft Dynamics CRM Entities" on page 1152).

   **Note:** CES 7.0.7433+ (February 2015) The incremental refresh supports deleted items.

3. Generate a field set, a mapping file, and an ObjectsToGet file with the Microsoft Dynamics CRM Connector Configuration Generator Tool (see "Using the Microsoft Dynamics CRM Connector Configuration Generator Tool" on page 1159).

4. In Coveo Administration Tool:
a. Configure the user identity

The connector needs to know the selected Microsoft Dynamics CRM account that you previously selected or created. Create a user identity (see "Adding a User Identity" on page 420).

b. CES 7.0.7599+ (April 2015) Configuring a security provider

When you want to index permissions, you must configure a security provider (see "Configuring a Microsoft Dynamics CRM Security Provider" on page 1163).

c. Create a Microsoft Dynamics CRM field set

Import the field set you generated previously with the Microsoft Dynamics CRM Connector Configuration Generator Tool to be able to easily add Microsoft Dynamics CRM specific facets to your Coveo search interfaces.

Note: By default, fields are not enabled as facets. You have to modify the field set after imported it.

d. Configure and index the Microsoft Dynamics CRM source

The Coveo connector needs to know details about the Microsoft Dynamics CRM system to be able to index its content (see "Configuring and Indexing a Microsoft Dynamics CRM Source" on page 1165).

e. (Optional) Modify hidden source parameters

Once your Microsoft Dynamics CRM source is up and running, if you encounter time out or performance issues, consider modifying some hidden source parameters to try resolving the issues (see "Modifying Hidden Microsoft Dynamics CRM Source Parameters" on page 1171).

9.26.3 Microsoft Dynamics CRM Connector Requirements

Your environment needs to meet the following requirements to be able to use the second generation Coveo connector for Microsoft Dynamics CRM systems:

- Coveo license for the Microsoft Dynamics CRM Connector

  Your Coveo license must include support for the Microsoft Dynamics CRM Connector to be able to use this connector.

- Microsoft Dynamics CRM On-Premises version 2013 or 2015, or Microsoft Dynamics CRM Online

  The connector was tested with Microsoft Dynamics CRM On-Premises (2013-2015) and Microsoft Dynamics CRM Online.

  Note: CES 7.0.7599+ (April 2015) Support for Microsoft Dynamics CRM 2015 On-Premises.

What's Next?

Choose or create a Microsoft Dynamics CRM account with which the connector will crawl the Microsoft Dynamics CRM content (see "Setting Up a Microsoft Dynamics CRM Full Read Account" on page 1155).
9.26.4 Enabling Auditing of Your Microsoft Dynamics CRM Entities

When you want to retrieve deleted items in your Microsoft Dynamics CRM system during a source incremental refresh, you must enable auditing on all indexed entities.

Notes:

- CES 7.0.7433 (February 2015) The incremental refresh supports deleted items.
- By default, auditing is disabled on all auditable entities.

To enable auditing of your Microsoft Dynamic CRM entities

1. Log in to the Microsoft Dynamics CRM with an account that has the System Administrator role.
2. Access the Auditing tab, by selecting in the nav bar Microsoft Dynamics CRM > Settings > Auditing.
3. In the Auditing tab, click Global Audit Settings.
4. In the System Settings window that appears:

   a. Under Audit Settings, click the Start Auditing check box.
   b. Under Enable Auditing in the following areas, for every indexed entities, click the [Entity] check box.
   c. Click OK.
5. Back in the Auditing tab, click Entity and Field Audit Settings.
6. In the **Solution: Default Solution** window that appears:

![Solution: Default Solution window](image)

   a. In the navigation panel on the left, select an entity (e.g., **Account**).

   b. In the right panel, in the **General** tab, ensure that under **Data Services**, the **Auditing** check box is selected.

   c. Repeat this procedure for every entities that you want to index.

   d. Save your modifications by clicking the **Save** icon.

   e. Publish your modifications by clicking **Publish**.

9.26.5 Microsoft Dynamics CRM Events Update Requirements

On a daily basis, users and administrators perform events in their Microsoft Dynamics CRM system(s) that can affect the content (e.g., add a comment on an article) and/or the security permissions (e.g., change the role of a user). Coveo administrators must thus schedule or perform (when urgent) the right source refresh type to retrieve all security permissions and content changes, keeping the index of their Microsoft Dynamics CRM source(s) up-to-date.

The following table provides a list of events in Microsoft Dynamics CRM and the required source refresh type to be scheduled or performed in the related Dynamics source(s).

<table>
<thead>
<tr>
<th>Event Description</th>
<th>Required Refresh Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Share a record with a user</td>
<td>Full refresh</td>
</tr>
<tr>
<td>Change the role of a user</td>
<td>Incremental refresh</td>
</tr>
</tbody>
</table>

**Example:** You share a record with a user, so you perform a source full refresh for the security permission change to be retrieved by the connector.

Events with an asterisk (*) character also require an update of the security cache.
Some events have no effect on security permissions and thus do not require a source refresh nor a security cache update.

**Note:** CES 7.0.7711+ (June 2015) The incremental refresh supports email and Sale Literature out-of-the-box attachments modifications (addition, edition). The source full refresh and rebuild support the deletion of email and Sale Literature out-of-the-box attachments starting with the same release.

<table>
<thead>
<tr>
<th>Event Name</th>
<th>Minimal Required Source Refresh Type</th>
<th>Security Cache Update</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Incremental Refresh</td>
<td>Full Refresh/Rebuild</td>
</tr>
<tr>
<td>Add a comment on an article</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Add a new record</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Add attachment on email</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Add attachment on Sale Literature</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Change hierarchy security manager/position</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Change ownership of a record</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Delete a related entity</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Enable/Disable hierarchy security</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Modify a record</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Modify a related entity record</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Modify an entity’s metadata</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Modify attachment on Sale Literature</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Submit/Approve/Unpublish a KB Article</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Update a comment on an article</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Delete attachment on email</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Delete attachment on Sale Literature</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Delete a comment on an article.</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Event Name</td>
<td>Minimal Required Source Refresh Type</td>
<td>Security Cache Update</td>
</tr>
<tr>
<td>-----------------------------------------------------</td>
<td>--------------------------------------</td>
<td>-----------------------</td>
</tr>
<tr>
<td></td>
<td>Incremental Refresh</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Full Refresh/Rebuild</td>
<td></td>
</tr>
<tr>
<td>Delete a sharing permission on a record</td>
<td>✔</td>
<td></td>
</tr>
<tr>
<td>Share a record</td>
<td>✔</td>
<td></td>
</tr>
<tr>
<td>Change the role of a user</td>
<td>✔</td>
<td></td>
</tr>
<tr>
<td>Change user of business unit</td>
<td>✔</td>
<td></td>
</tr>
<tr>
<td>Modify manager/position of a user</td>
<td>✔</td>
<td></td>
</tr>
<tr>
<td>Modify position hierarchy</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Auditing is enabled/disabled for an entity</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Auditing is enabled/disabled on the organization</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**9.26.6 Setting Up a Microsoft Dynamics CRM Full Read Account**

The Coveo Dynamics CRM connector needs to connect to the Microsoft Dynamics CRM system using an account that has read access to all the Microsoft Dynamics CRM content that you want to index.

The Coveo connector only reads and does not modify Microsoft Dynamics CRM content. Consequently, you could create and use a dedicated account for the Coveo connector. This account would have full read (but not write) access to the Microsoft Dynamics CRM content that you want to index and would be used only by the Coveo connector. The following procedure describes how to create such an account in Microsoft Dynamics CRM 2013 On-Premises.

**Creating a dedicated user account with full read rights (Dynamics 2013 On-Premises)**

1. Using a network administrator account or asking your network administrator, create a Windows account for a dedicated Microsoft Dynamics CRM crawling user.

   **Important:** Microsoft Dynamics requires that the account has a first name and a last name. These parameters must not be empty.

2. Log in to the Microsoft Dynamics CRM 2013 with an account that has the System Administrator role, and then perform the following steps.

3. Copy the System Administrator security role:
a. On the nav bar, click **Microsoft Dynamics CRM > Settings**.

b. Still on the nav bar, click **Settings > Administration**.

c. In the **Administration** page, click **Security Roles**.

d. In the **Security Roles** page, select the **System Administrator** security role.

e. In the **Security Role: System Administrator** window, on the menu, click **Actions**, and then click **Copy Role**.

f. In the **Copy Security Role** dialog box, in the **New Role Name** box, type a new role name of your choice such as **Read-Only Administrator**.

g. Select the **Open a new security role when copying is complete** check box.

h. Click **OK**.

4. In the **Security Role** window that appears for the new role:

a. Select the **Core Records** tab.

b. Set all rights to **None Selected** except for those in the **Read** column.

   **Note:** Only select the Read right for the entities you want to index.

   **Tip:** Click the label of a column to change the rights of all column items at once.
c. Set similar rights for all the other tabs.

d. On the bar at the top of the window, click **Save and Close**.

5. Create a new user using the user created in step 1:

a. On the nav bar, click **Settings > Administration**.

b. In the **Administration** page, click **Users**.

c. In the options above **Enabled Users**, click **New**.

d. In the **New User** page, in the **Summary** section:

   i. In the **User Name** box, enter the user created in step 1 in the form `username@domain`.

   ii. In the **Full Name** box, enter any **First Name** and **Last Name**.

e. In the options above **Enabled Users**, click **Save**.

6. Assign the role you just created to this user:

   a. In the page for the new user, in the options at the top, click more commands button, and then click **Manage Roles**.
b. In the **Manage User Roles** dialog box:
   
   i. Select the check box for the role that you created in step 4 (**Read-Only Administrator** in the example) and clear all other check boxes.
   
   ii. Click **OK**.

c. In the **Confirm Security Role Assignment** dialog box:

   i. Select the check box for the role that you created in step 4 (**Read-Only Administrator** in the example) and clear all other check boxes.

   ii. Click **OK**.
What's Next?

Generate the necessary configuration files (see "Using the Microsoft Dynamics CRM Connector Configuration Generator Tool" on page 1159).

9.26.7 Using the Microsoft Dynamics CRM Connector Configuration Generator Tool

The Dynamics Configuration Generator is a tool used to generate all the necessary configuration files for a specific Microsoft Dynamics CRM Organization, in order to index it properly.

To use the Microsoft Dynamics CRM Connector Configuration Generator Tool

1. Get your Discovery Service URL and Organization Name:
   a. Log into Microsoft Dynamics CRM Organization with an administrator account.
   b. Access the Developers Resources page:
      i. Click the Microsoft Dynamics CRM drop-down menu in the top-left of the screen, and then select Settings.
      ii. Click the Settings drop-down menu, and then select Customizations.
      iii. In the Customization page, click Developers Resources.
   c. In the Developers Resources page, take note of your Organization Unique Name and Discovery Service URL.
Example: In Microsoft Dynamics CRM 2103 On-Premises, the **Developers Resources** page looks like the following:

2. Open the Microsoft Dynamics CRM Connector Configuration Generator Tool located in the CES 7 Bin folder.

    Example: C:\Program Files\Coveo Enterprise Search 7\Bin\DynamicsConfigGenerator.exe

3. In the **Microsoft Dynamics CRM Connector Configuration Generator Tool** interface:
a. Under **Configuration:**

   i. In the **Discovery Service URL** box, enter the full discovery service endpoint URL.

   ii. In the **Organization Name** box, enter the organization unique name.

   iii. In the **User Name** and **Passwords** boxes, enter the credentials of the administrator account you previously used to create a user identity (see Microsoft Dynamics CRM Connector Deployment Overview).

   iv. Click **Connect**.

   The connection to the Organization is initialized, displaying any errors and retrieving the complete entities schema. Retrieving the schema can take some time to complete.
Notes:

- After receiving the schema, a list of entities will be displayed in the left panel. For a better experience, the tool does not show entities that are not customizable. These entities are normally system entities with no relevant data.

- CES 7.0.7599+ (April 2015) Meaningful entities and their attributes are selected by default.

b. In the left panel, select the check box next to the entities you want to index.

**Note:** Your selection defines the content of the ObjectsToGet file. The connector uses this file to determine what type of entity to get and what attributes to retrieve as their metadata.

c. For each selected entities check boxes:

i. Click an entity row.

ii. In the **Entity Information** tab, in the **Attributes** section panel on the right, select the attribute(s) to be used to create a corresponding field in the field set.

**Note:** Each attribute for a specific entity will also be added in the document’s metadata with the corresponding value.

iii. Finish configuring the mapping file:

**Note:** The mapping file is generated using the selected entities and the entered **Title** and **Body** mappings (if any).

In the **Title** and **Body** boxes:

- Enter the exact same attribute name(s) selected in step ii in the format `%[AttributeName].`

**Note:** In the **Attributes** section, the name in parentheses represents the name of the attribute in the mapping file.

**Example:**

In the **Title** box, when you selected the **Accountid** attribute, enter `%[Accountid].`

In the **Body** box, when you selected the **Description** attribute, enter `%[Description].`

OR

- Drag-and-drop attribute(s).

iv. CES 7.0.7599+ (April 2015) Click the **Relations** tab to setup entity relations.

v. In the **Relations** tab, for each selected related entities:

A. Select the attribute(s) to be added to the current entity’s metadata and used to create a corresponding field in the field set.
Note: Each attribute for a specific entity is added in the document's metadata with the corresponding value in the following format:

[ALIAS]. [ATTRIBUTE_NAME]

Example: When the alias is primarycontact and you select the Account attribute, the field that will be created in the field set is primarycontact.Account.

B. (Optionally) Rename the Alias.

Note: Adding relations can have a significant impact on crawling performances.

d. Click Save to files.

e. In the notification prompt that appears, select an output folder, and then click OK.

Three configuration files are generated and prefixed by the unique name of your Organization.


What's Next?

Configure and index a Microsoft Dynamics CRM source (see "Configuring and Indexing a Microsoft Dynamics CRM Source" on page 1165).

9.26.8 Configuring a Microsoft Dynamics CRM Security Provider

CES 7.0.7599+ (April 2015)

The Microsoft Dynamics CRM connector needs a security provider to manage the user permissions on Microsoft Dynamics CRM entities. The Microsoft Dynamics CRM security provider performs tasks such as expanding groups to users and mapping Microsoft Dynamics CRM users to emails or to Active Directory users. The connector creates and sets several virtual groups on indexed documents to support the access policies defined in Microsoft Dynamics CRM.

Note: You can get familiar with how Coveo components deal with permissions on documents both at indexing and query time.

To Configure a Microsoft Dynamics CRM security provider

1. On the Coveo server, access the Administration Tool.


3. In the Security page, in the navigation panel on the left, click Security Providers.

4. In the Security Providers page, click Add to create a new security provider.

5. In the Modify Security Provider page:
a. In the **Name** box, enter a name to identify this security provider.

**Example**: Microsoft Dynamics CRM Security Provider

b. In the **Security Provider Type** drop-down list, select **Microsoft Dynamics CRM**.

**Note**: If you do not see Microsoft Dynamics CRM in the Security Provider Type list, your environment does not meet the requirements (see "Microsoft Dynamics CRM Connector Requirements" on page 1151).

c. In the **User Identity** section:

   i. In the drop-down list, select the user identity that you created previously with the Microsoft Dynamics CRM crawling account credentials (see Microsoft Dynamics CRM Connector Deployment Overview).

   ii. When needed, click **Add**, **Edit**, or **Manage user identities** respectively to create, modify, or manage user identities.

d. In the **Organization unique name** box, enter the same unique name of the organization you previously entered (see Using the Microsoft Dynamics CRM Connector Configuration Generator Tool).

e. In the **Discovery server URL** box, enter the root address of your Microsoft Dynamics CRM organization.

   - For an on-premises setup (CRM 2013-2015 On-Premises), enter the Discovery Service hosted on
the server. You can find this URL in your Microsoft Dynamic CRM system using the Configuration generator tool (see Using the Microsoft Dynamics CRM Connector Configuration Generator Tool).

**Note:** You only need to put the URL of the server, the connector will add /XRMServices/2011/Discovery.svc to the starting address.

**Example:** When your Discovery Service URL is http://MyDynamicsServer/XRMServices/2011/Discovery.svc, enter http://MyDynamicsServer in the Addresses box.

- For an online setup (CRM Online), enter the correct server depending on your location (see Discover the URL for your organization with IDiscoveryService web service).

**Example:** When your Organization is hosted in North-America, enter https://disco.crm.dynamics.com/.

**Note:** When you want to index more than one Microsoft Dynamics CRM server or more than one organization, the best practice is to enter only one address here, for one server/organization and create other sources for other server/organizations.

f. In the Security Provider drop-down list, for a Microsoft Dynamics CRM On-Premises organization, select Active Directory or a custom Active Directory security provider that you created for your specific domain (see "Configuring an Active Directory Security Provider" on page 1141).

**Notes:**

- Users in your Microsoft Dynamics CRM On-Premises organization must match the users in your Active Directory.

- For a Microsoft Dynamics CRM Online organization, contact Coveo Professional Services to configure a customized security provider for your setup.

g. Leave the Allow Complex Identities option cleared as it does not apply to this type of security provider.

h. Click Apply Changes.

What's Next?

Configure and index your Microsoft Dynamics CRM source (see "Configuring and Indexing a Microsoft Dynamics CRM Source" on page 1165).

9.26.9 Configuring and Indexing a Microsoft Dynamics CRM Source

A source defines a set of configuration parameters for a specific Microsoft Dynamics CRM system.

**Note:** In an environment with more than one Microsoft Dynamics CRM system, or more than one Microsoft Dynamics CRM organization, you need to define one source for each Microsoft Dynamics CRM organization that you want to index.
To configure and index a Microsoft Dynamic CRM source

1. On the Coveo server, access the Administration Tool.

2. Select **Index > Sources and Collections**.

3. In the **Collections** section:
   a. Select an existing collection in which you want to add the new source.
   OR
   b. Click **Add** to create a new collection.

4. In the **Sources** section, click **Add**.

   The **Add Source** page that appears is organized in three sections.

5. In the **General Settings** section of the **Add Source** page:

   a. Enter the appropriate value for the following required parameters:

   **Name**

   Enter a descriptive name of your choice for the connector source.

   **Example:** Dynamics CRM
Source Type

Select the connector used by this source. In this case, select Dynamics CRM.

**Note:** If you do not see Dynamics CRM in the Source Type list, your environment does not meet the requirements (see "Microsoft Dynamics CRM Connector Requirements" on page 1151).

Addresses

The root address of the Microsoft Dynamics CRM organization.

- For an on-premises setup (CRM 2013-2015 On-Premises), enter the Discovery Service hosted on the server. You can find this URL in your Microsoft Dynamic CRM system using the Configuration generator tool (see Using the Microsoft Dynamics CRM Connector Configuration Generator Tool).

**Notes:**

- You only need to put the URL of the server, the connector will add /XRMServices/2011/Discovery.svc to the starting address.

  **Example:** When your Discovery Service URL is http://MyDynamicsServer/XRMServices/2011/Discovery.svc, enter http://MyDynamicsServer in the Addresses box.


- For an online setup (CRM Online), enter the correct server depending on your location (see Discover the URL for your organization with IDiscoveryService web service).

  **Example:** When your Organization is hosted in North-America, enter https://disco.crm.dynamics.com/.

**Note:** When you want to index more than one Microsoft Dynamics CRM server or more than one organization, the best practice is to enter only one address here, for one server/organization and create other sources for other server/organizations.

Refresh Schedule

Time interval at which the index is automatically refreshed to keep the index content up-to-date. By default, the **Every day** option instructs CES to refresh the source everyday at 12 AM.

**Notes:**

- Auditing must be enabled for indexed entities for the connector to be able to retrieve deleted items during an incremental refresh (see "Enabling Auditing of Your Microsoft Dynamics CRM Entities" on page 1152).

- You can create new or modify existing source refresh schedules.

b. Review the value for the following parameters that often do not need to be modified:
Rating

Change this value only when you want to globally change the ranking associated with all items in this source relative to the rating of other sources.

Example: If this source was for a legacy system, you may want to set this parameter to Low, so that in the search interface, results from this source appear later in the list compared to those from other sources.

Document Types

If you created a custom document type set for this source, select it. Otherwise, select Default.

Active Languages

If you defined custom active language sets, ensure to select the most appropriate for this source.

Fields

Select the custom field set you previously defined (see Microsoft Dynamics CRM Connector Deployment Overview).

6. In the Specific Connector Parameters & Options section of the Add Source page:

   a. In the Organization Unique name box, enter the same unique name of the organization you previously entered (see Using the Microsoft Dynamics CRM Connector Configuration Generator Tool).

   b. In the ObjectsToGet File Path box, enter the absolute full path pointing to the connector ObjectsToGet file that you previously generate (see "Using the Microsoft Dynamics CRM Connector Configuration Generator Tool" on page 1159). Click next to the box to open a browsing dialog box to easily select the file.

      Example: C:\Program Files\Coveo Enterprise Search 7\Bin\[MyUniqueOrganizationName]ObjectsToGet.xml

   c. In the Mapping File box, enter the absolute full path pointing to the connector mapping file that you previously generated (see "Using the Microsoft Dynamics CRM Connector Configuration Generator Tool"
on page 1159). Click next to the box to open a browsing dialog box to easily select the file.

**Example:** C:\Program Files\Coveo Enterprise Search 7\Bin\[MyUniqueOrganizationName]MappingFile.xml

d. In the **Parameters** section, click **Add Parameter** when you want to show advanced source parameters (see "Modifying Hidden Microsoft Dynamics CRM Source Parameters" on page 1171).

e. The **Option** check boxes generally do not need to be changed:

**Index Subfolders**

- Leave check box cleared. The connector for this type of source does not use this parameter.

**Index the document’s metadata**

When selected, CES indexes all the document metadata, even metadata that are not associated with a field. The orphan metadata are added to the body of the document so that they can be searched using free text queries.

When cleared (default), only the values of system and custom fields that have the **Free Text Queries** attribute selected will be searchable without using a field query.

**Example:** A document has two metadata:

- **LastEditedBy** containing the value Hector Smith
- **Department** containing the value RH

In CES, the custom field **CorpDepartment** is bound to the metadata **Department** and its **Free Text Queries** attribute is selected.

When the **Index the document’s metadata** option is cleared, searching for **RH** returns the document because a field is indexing this value. Searching for **hector** does not return the document because no field is indexing this value.

When the **Index the document’s metadata** option is selected, searching for **hector** also returns the document because CES indexed orphan metadata.

**Document’s addresses are case-sensitive**

- Leave the check box cleared. This parameter needs to be checked only in rare cases for systems in which distinct documents may have the same name but different casing.

**Generate a cached HTML version of indexed documents**

- When you select this check box (recommended), at indexing time, CES creates HTML versions of indexed documents. In the search interfaces, users can then more rapidly review the content by clicking the Quick View link rather than opening the original document with the original application. Consider clearing this check box only if you do not want to use Quick View links or to save resources when building the source.
Open results with cached version

Leave this check box cleared (recommended) so that in the search interfaces, the main search result link opens the original document with the original application. Consider selecting this check box only when you do not want users to be able to open the original document but only see the HTML version of the document as a Quick View. In this case, you must also select Generate a cached HTML version of indexed documents.

7. In the Security section of the Add Source page:

   [Image of Security section]

   a. In the Authentication drop-down list, select the user identity that you created for the Microsoft Dynamics CRM system.

   b. In the Security Provider drop-down list:

      - **CES 7.0.7599+ (April 2015)** Select the Microsoft Dynamics CRM security provider that you created for this source (see Microsoft Dynamics CRM Connector Deployment Overview).

      - **CES 7.0.7433– (February 2015)** Select (none).

      **Important: CES 7.0.7433– (February 2015)** The connector does not support Microsoft Dynamics CRM 2013 On-Premises and Online permissions. It is thus strongly recommended to only index public Dynamics CRM system(s).

      **Note:** A workaround is to manually define permissions on the source (see Permissions).

   c. Click Save and Start to save the source configuration and start indexing this source.

7. When you choose to not index permissions associated with Microsoft Dynamics CRM items:

   **Important: CES 7.0.7433– (February 2015)** The connector does not support Microsoft Dynamics CRM 2013 On-Premises and Online security model (role-based and object-based permissions). This means that, in the Coveo search interface, a user searching Microsoft Dynamics CRM content could see content to which he has normally no access in the Microsoft Dynamics CRM system.

   **Note:** When your Microsoft Dynamics CRM system content is not public, a workaround is to enter the name of user(s) or group(s) you want to allow or deny access to your organization content in the Allowed Users and Deny Users boxes.
a. In the navigation menu on the left, select **Permissions**.

b. Next to **Permissions**, select the **Specifies the security permissions to index** option.

c. Next to **Allowed Users**, ensure that a well-known everyone group such as the Active Directory everyone \S-1-1-0\ is added.

d. Click **Apply Changes**.

9. Validate that the source building process is executed without errors:

   - In the navigation panel on the left, click **Status**, and then validate that the indexing proceeds without errors.

   OR

   - Open the CES Console to monitor the source building activities.

What's Next?

Set an incremental refresh schedule for your source.

9.26.9.1 Modifying Hidden Microsoft Dynamics CRM Source Parameters

The **Add Source** and **Source: ... General** pages of the Administration Tool present the parameters with which you can configure the connector for most Microsoft Dynamics CRM setups. More advanced and more rarely used
parameters are hidden. You can choose to make one or more of these parameters appear in the Add Source and Source: ... General pages of the Administration Tool so that you can change their default value. Consider changing values of hidden parameters only when you encounter time out error messages or performance issues.

The following list describes the available advanced hidden parameters for Microsoft Dynamics CRM sources. The parameter type (integer, string,...) appears between parentheses following the parameter name.

**DiscoveryServiceUrl (String)**

The discovery service URL. The default value is the starting address added with "/XRMServices/2011/Discovery.svc", which should be the same for all Microsoft Dynamics CRM instances.

| Note: This parameter is only required when you need to override the /XRMServices/2011/Discovery.svc part. |

**RecordsPageSize (Integer)**

Number of records to retrieve per request. A bigger batch size will put more stress on the server but less on the network. The default value is 250 records.

Use the following procedure only when you want to modify one or more of the above hidden source parameters.

To modify hidden Microsoft Dynamics CRM source parameters

1. Refer to "Adding an Explicit Connector Parameter" on page 450 to add one or more Microsoft Dynamics CRM hidden source parameters.

2. For a new Microsoft Dynamics CRM source, access the Add Source page of the Administration Tool to modify the value of the newly added advanced parameter:
   a. Select Index > Sources and Collections.
   b. Under Collections, select the collection in which you want to add the source.
   c. Under Sources, click Add.
   d. In the Add Source page, edit the newly added advanced parameter value.

3. For an existing Microsoft Dynamics CRM source, access the Source: ... General page of the Administration Tool to modify the value of the newly added advanced parameter:
   a. Select Index > Sources and Collections.
   b. Under Collections, select the collection containing the source you want to modify.
   c. Under Sources, click the existing Microsoft Dynamics CRM source in which you want to modify the newly added advanced parameter.
   d. In the Source: ... General page, edit the newly added advanced parameter value.
9.26.10 Troubleshooting Microsoft Dynamics CRM Connector Issues

Microsoft Dynamics CRM search results have no related metadata

Possible cause
You update a version prior to CES 7.0.7711 (June 2015 release) to the CES 7.0.7711 version or subsequent.

Possible solution
Metadata name was changed to better match metadata available on Microsoft Dynamics CRM documents following the CES 7.0.7711 June 2015 release. You must thus regenerate the Dynamics source configuration files (mapping file, field set, objects to get) with the generator tool, and then rebuild your Dynamics source (see "Using the Microsoft Dynamics CRM Connector Configuration Generator Tool" on page 1159 and "Applying an Action to a Collection or a Source" on page 283).

9.27 Microsoft Exchange Connector

The Coveo connector for Microsoft Exchange systems allows Coveo administrators to bring the content of Exchange mailboxes, mailbox archives, and public folders into the unified index so that they become searchable by end-users.

9.27.1 Connector Features Summary

<table>
<thead>
<tr>
<th>Features</th>
<th>Supported</th>
<th>Additional information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Exchange version</td>
<td>2010, 2013, 2016, and Online</td>
<td>(For Exchange Online only) Following available Exchange Online releases</td>
</tr>
<tr>
<td>Searchable content types</td>
<td>✅</td>
<td>Emails, attachments, and events</td>
</tr>
<tr>
<td>Content update</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Incremental refresh</td>
<td>✅</td>
<td></td>
</tr>
<tr>
<td>Full refresh</td>
<td>✅</td>
<td></td>
</tr>
<tr>
<td>Rebuild</td>
<td>✅</td>
<td></td>
</tr>
<tr>
<td>Document-level security</td>
<td>✗</td>
<td>Permissions must be manually defined on the source</td>
</tr>
</tbody>
</table>

9.27.2 Features

The Microsoft Exchange connector features are:
- Support for Microsoft Exchange 2016, 2013, 2010, and Online servers

**Notes:**
- **CES 7.0.8047+ (December 2015)** The connector supports Microsoft Exchange 2016.
- **CES 7.0.5425+ (May 2013)** The connector supports Microsoft Exchange 2013.
- **CES 7.0.7814+ (August 2015)** The connector can index Microsoft Exchange Online mailboxes (not only remote archives).
- **CES 7.0.7711–(June 2015)** The connector could not index Exchange Online on an organization-wide basis due to Microsoft API limitations.

- **CES 7.0.6684+ (May 2014)** In the context of an Exchange Server 2013 hybrid deployment, support for remote archives hosted in Exchange Online
- Support Web Services and WebDAV connection types
- Mailbox indexing
- Lync conversation history indexing
- Microsoft Exchange 2013/2010 mailbox archive indexing
- Public folder indexing
- Security indexing combining:
  - Microsoft Exchange permissions set in Exchange by users
  - Permissions set in Active Directory by administrators
- Incremental refresh to periodically query Microsoft Exchange for the latest edits, keeping the index content up-to-date
- Metadata collecting for emails, contacts, tasks, and calendars
- Supports two types of forms-based authentication for Outlook Web Access (OWA):
  - Standard Exchange forms-based authentication
  - ISA Server forms-based authentication
- Support for the standard Microsoft Exchange front-end and back-end server configurations (as described in the Microsoft articles Front-End and Back-End Topologies Overview and Front-End and Back-End Topology Advantages).
- **CES 7.0.8047+ (December 2015)** When indexing Exchange content, the connector can be paused and resumed if an hidden parameter is set (see Modifying Hidden Microsoft Exchange Source Parameters).
Feature History

<table>
<thead>
<tr>
<th>Coveo Platform version</th>
<th>Monthly release</th>
<th>Features</th>
</tr>
</thead>
<tbody>
<tr>
<td>7.0.8047</td>
<td>December 2015</td>
<td>Support for Microsoft 2016.</td>
</tr>
<tr>
<td>7.0.7814</td>
<td>August 2015</td>
<td>Indexing of Exchange Online mailboxes (see &quot;Configuring and Indexing Microsoft Exchange Sources for an Online Deployment&quot; on page 1215).</td>
</tr>
<tr>
<td>7.0.6684</td>
<td>May 2014</td>
<td>In the context of an Exchange Server 2013 hybrid deployment, support for remote archives hosted in Exchange Online (see &quot;Configuring and Indexing Microsoft Exchange Sources for a Hybrid Deployment&quot; on page 1207).</td>
</tr>
<tr>
<td>7.0.6607</td>
<td>April 2014</td>
<td>For Exchange 2013 search results, breadcrumbs show full email folder hierarchy.</td>
</tr>
<tr>
<td>7.0.5425</td>
<td>May 2013</td>
<td>Support for Microsoft Exchange 2013</td>
</tr>
</tbody>
</table>

What's Next?

Review the steps for the deployment of the Microsoft Exchange connector (see "Microsoft Exchange Connector Deployment Overview" on page 1175).

9.27.3 Microsoft Exchange Connector Deployment Overview

The following procedure outlines the steps needed to deploy the Microsoft Exchange connector. The steps indicate the order in which you must perform configuration tasks on both the Microsoft Exchange and CES systems. Some steps are applicable only to particular Exchange deployment configurations.

About the Support for Exchange Server 2013 Hybrid Deployments

In the context of an Exchange Server 2013 hybrid deployment, the Coveo connector supports to index the following content:

- Local full content (mailboxes, archives, public folders) on the Exchange On-Premises Server 2013
- Remote archives on Exchange Online

As you can see local is relative to the Exchange On-Premises Server. Archives can be both local when on the On-Premises server, or remote when on Exchange Online.

In the context of an Exchange Server 2013 hybrid deployment, as indicated in the following procedure, you must create two sources, respectively for the local and remote parts.

**Note:** CES 7.0.6684+ (May 2014) Support for indexing remote archives in the context of an Exchange Server 2013 hybrid deployment.
To deploy the Microsoft Exchange connector

1. Validate that your environment meets the requirements (see "Microsoft Exchange Connector Requirements" on page 1178).

2. Microsoft Exchange configuration:
   a. Create the Exchange crawling account to be used by the Coveo connector to access your Exchange content (see "Creating a Microsoft Exchange Crawling Account" on page 1183).
   b. For Microsoft Exchange Server 2010 only:
      i. Configure the throttling policy (see "Configuring the Throttling Policy for the Microsoft Exchange Account" on page 1190).
      ii. When you plan to index Exchange public folders, ensure that the public folders of your users are correctly configured for the crawler (see "Preventing Microsoft Exchange Public Folder Crawling Issues" on page 1192).
   c. For an Exchange hybrid deployment only, when you want to index remote archives, you must enable impersonation for the CES crawling identity in Exchange Online (see "Enabling Impersonation in Microsoft Exchange Online" on page 1193).
   d. CES 7.0.7814+ (August 2015) For an Exchange Online deployment with cloud-based users only, authorize the Coveo connector to access the online mailboxes of your Azure AD users (see "Authorizing the Coveo Connector to Access the Exchange Online Mailboxes of Your Azure AD Users" on page 1186).

3. On the Coveo server, in the Administration Tool:
   a. Configure the user identity.
      The connector needs to know the credentials of the Microsoft Exchange account that you created in step 2.a by creating a CES user identity that you will later associate to your Microsoft Exchange source (see "Adding a User Identity" on page 420).
   b. Configure a security provider that you will later associate to your Microsoft Exchange source.
      Depending on your kind of deployment:
      - For hybrid or on-premises deployments
         The connector needs information on how to manage Microsoft Exchange permissions (see "Configuring a Microsoft Exchange Security Provider" on page 1194).
      - CES 7.0.7814+ (August 2015) For online deployments with cloud-based users
         Since the Azure AD Graph API used to list the Microsoft Exchange Online mailboxes is not an Exchange API, it is currently not possible to retrieve Exchange permissions on indexed items. Thus, only the owner of the mailbox, whom identity is either his principal email address or his UPN (UserPrincipalName), is allowed to see his documents.
Starting with the owner identity of each mailbox, the security provider type to use depends on how users are authenticated when they access the Coveo search interface:

**Notes:**

- The members retrieved on documents are going to be mapped to this security provider identity type.
- You may require to also use a REGEX Transform Member Name security provider in between the two security providers presented below to map member types. Contact Coveo Support for assistance.

- When authenticated with their email address, use an Email security provider (see "Configuring an Email Security Provider" on page 65).
- When authenticated with an Active Directory account, use an Active Directory security provider (see "Configuring an Active Directory Security Provider" on page 1141).

**Notes:**

- CES comes with an Active Directory security provider that you can configure to connect to the default domain. When your environment contains more than one domain, you can select an Active Directory security provider that you created for other domains.
- An Active Directory security provider is appropriate only when the User Principal Name (UPN) matches the email address for all users.

c. Configure and index the Microsoft Exchange source.

The Coveo connector needs to know details about the Microsoft Exchange Server or hybrid deployment to be able to index its content.

- When indexing only an Exchange On-Premises Server, see "Configuring and Indexing a Microsoft Exchange Source for an On-Premises Deployment" on page 1197.

- When indexing an Exchange Server 2013 hybrid deployment, see "Configuring and Indexing Microsoft Exchange Sources for a Hybrid Deployment" on page 1207.

- **CES 7.0.7814+ (August 2015)** When indexing Exchange Online mailboxes, see "Configuring and Indexing Microsoft Exchange Sources for an Online Deployment" on page 1215.

d. Optionally, modify hidden source parameters.

Once your Microsoft Exchange source is up and running, if you encounter indexing issues, consider modifying some hidden source parameters to try resolving the issues (see "Modifying Hidden Microsoft Exchange Source Parameters" on page 1222).

e. Optionally, fine-tune the callback service

For Microsoft Exchange Server 2013, 2010, and 2007, the Coveo Exchange (WebServices) connector uses an Exchange API to identify modified content and improve incremental refresh performances. You can fine-tune the callback service configuration file (see "Fine-Tuning the Exchange Callback Service" on page 1204).
What's Next?

In out-of-the-box Coveo .NET search interfaces, end-users can select to open Exchange email search results either in Outlook Web Access (OWA) or directly in Outlook from Coveo .NET search interfaces using the Open emails with Microsoft Outlook search interface preference option.

- With Outlook 2007 and up on Windows systems, the outlook:// protocol is disabled by default when Microsoft Office is installed. The email result links in Coveo search interfaces use this protocol to allow users to open email search results directly in Outlook. If not already done, enable the protocol on all workstations for example using GPO (see Shortcuts and the Missing Outlook:// Protocol).

- If not already done, consider deploying the Desktop Integration Package on workstations to allow users to take advantage of the Outlook Sidebar.

9.27.4 Microsoft Exchange Connector Requirements

Your environment needs to meet the following requirements to be able to use the Coveo connector for Microsoft Exchange systems:

- Coveo license for the Microsoft Exchange Connector

  Your Coveo license must include support for the Microsoft Exchange Connector to be able to use this connector.

- Microsoft Exchange versions:
  - Supported versions:
    - Online
    - 2010, 2013 (on-premises or hybrid), 2016

  Notes:
  
  - CES 7.0.7814+ (August 2015) Support for Microsoft Exchange Online mailboxes.
  - CES 7.0.6684+ (May 2014) Support for indexing remote archives hosted in Exchange Online in the context of an Exchange Server 2013 hybrid deployment.

  - Deprecated support versions: 2003, 2007 SP1

What's Next?

Set up a full read Microsoft Exchange Account (see "Setting up a Full Read Microsoft Exchange Account" on page 1185).

9.27.5 Microsoft Exchange Online Source Quick Setups

**CES 7.0.7814+ (August 2015)**

The Coveo connector for Exchange now supports three different Exchange Online setups (see "Microsoft Exchange Connector" on page 1173). Consequently, the Coveo components and parameter values required to create Exchange Online sources vary depending on the Exchange Online environment.
The configuration of the components required to create a source for a given common Exchange environment is however often simple for an administrator that is familiar with the Coveo Enterprise Search (CES) source creation process.

The topics in this section outline the required components and parameters to create a source for the supported Exchange Online environments. Parameters not mentioned should be left to their default values.

In the table of contents, each quick setup title gives information on the Exchange Online environment, helping you choosing the quick setup that best suits your needs.

9.27.5.1 Microsoft Exchange Online With Azure AD Users (Cloud-Based or Synced/Federated) Source Quick Setup

**CES 7.0.7814+ (August 2015)**

This topic outlines the required components and parameters to create a source for an Exchange Online deployment where:

- All mailboxes are stored in Exchange Online
- Mailbox owners are:
  - Cloud-based users that can be listed using Azure AD.
  - Federated users synced in Azure AD.

Parameters not mentioned should be left to their default values.

1. Validate that your environment meets the requirements:
   - **CES 7.0.7814+ (August 2015)**
   - Your Coveo license includes the Microsoft Exchange Connector.

2. Create a user identity with a dedicated Windows account that has access to all the Exchange content that you want to index. [more]

<table>
<thead>
<tr>
<th>Key parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Name</strong></td>
<td>You must name your user identity.</td>
</tr>
<tr>
<td><strong>User</strong></td>
<td>An Office 365 Administrator account that can access your Windows Azure management portal.</td>
</tr>
<tr>
<td><strong>Password</strong></td>
<td>The corresponding password.</td>
</tr>
</tbody>
</table>

3. In the Windows Azure management portal, create an Azure AD application to authorize the Coveo connector to access the Exchange Online mailboxes of your Azure AD users. [more]

4. Depending on the way your users authenticate in your Coveo search interface, create a security provider to
resolve Azure AD users. [more]

- When authenticating with an email:

<table>
<thead>
<tr>
<th>Key parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>You must name your security provider.</td>
</tr>
<tr>
<td>Security Provider Type</td>
<td>Email</td>
</tr>
<tr>
<td>Security Provider</td>
<td>(Optional) The security provider to map Email identities to another identity type.</td>
</tr>
</tbody>
</table>

- When authenticating with an AD account, use the default Active Directory security provider or create a new one:

  **Important:** The User Principal Name (UPN) must match the email address for all users.

<table>
<thead>
<tr>
<th>Key parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>You must name your security provider.</td>
</tr>
<tr>
<td>Security Provider Type</td>
<td>Active Directory</td>
</tr>
<tr>
<td>User Identity</td>
<td>The user identity containing an account that has access to the desired domain or (none) when you want to use the CES service account.</td>
</tr>
<tr>
<td>Security Provider</td>
<td>(Optional) The security provider to map Email identities to another identity type.</td>
</tr>
</tbody>
</table>

5. Create an Exchange source. [more]

<table>
<thead>
<tr>
<th>Key parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>You must name your source.</td>
</tr>
<tr>
<td>Source Type</td>
<td>Exchange (WebServices)</td>
</tr>
<tr>
<td>Addresses</td>
<td><a href="https://outlook.office365.com/">https://outlook.office365.com/</a></td>
</tr>
<tr>
<td>AzureAdOAuth2TokenEndpoint (hidden parameter)</td>
<td>The endpoint used to obtain an access token using OAuth 2.0 (see Authorizing the Coveo Connector to Access the Exchange Online Mailboxes of Your Azure AD Users).</td>
</tr>
</tbody>
</table>
### Key parameter | Value
--- | ---
**AzureAdGraphApiEndpoint** (hidden parameter) | The endpoint used by the Azure AD Graph API to access directory data in the Windows Azure AD directory (see Authorizing the Coveo Connector to Access the Exchange Online Mailboxes of Your Azure AD Users).

**AzureAdClientId** (hidden parameter) | The Azure AD client ID you previously obtained (see Authorizing the Coveo Connector to Access the Exchange Online Mailboxes of Your Azure AD Users).

**AzureAdClientKey** (hidden parameter) | The Azure AD client key you previously obtained (see Authorizing the Coveo Connector to Access the Exchange Online Mailboxes of Your Azure AD Users).

**OwnerOnlySecurity** (hidden parameter) | true

**Exchange Security Provider** | The security provider you just created.

**Authentication** | The user identity you created.

---

### 9.27.5.2 Microsoft Exchange Online With Federated Users Source Quick Setup

**CES 7.0.7814+ (August 2015)**

This topic outlines the required components and parameters to create a source for an Exchange Online deployment where:

- All mailboxes are stored in Exchange Online
- Mailbox owners are on-premises users listed in a local AD.

Parameters not mentioned should be left to their default values.

1. **Validate that your environment meets the requirements:**
   - **CES 7.0.7814+ (August 2015)**
   - Your Coveo license includes the Microsoft Exchange Connector.

2. **Create a user identity with a dedicated Windows account that has access to all the Exchange content that you want to index.** [more]

### Key parameter | Value
--- | ---
**Name** | You must name your user identity.
<table>
<thead>
<tr>
<th>Key parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>User</td>
<td>A full read Microsoft Exchange account that has read access on all the mailboxes you want to index.</td>
</tr>
<tr>
<td>Password</td>
<td>The corresponding password.</td>
</tr>
</tbody>
</table>

3. Depending on the way your users authenticate in your Coveo search interface, create a security provider to resolve AD users. [more]

- When authenticating with an email:

<table>
<thead>
<tr>
<th>Key parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>You must name your security provider.</td>
</tr>
<tr>
<td>Security Provider Type</td>
<td>Email</td>
</tr>
<tr>
<td>Security Provider</td>
<td>(Optional) The security provider to map Email identities to another identity type.</td>
</tr>
</tbody>
</table>

- When authenticating with an AD account, use the default Active Directory security provider or create a new one:

  **Important:** The User Principal Name (UPN) must match the email address for all users.

<table>
<thead>
<tr>
<th>Key parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>You must name your security provider.</td>
</tr>
<tr>
<td>Security Provider Type</td>
<td>Active Directory</td>
</tr>
<tr>
<td>User Identity</td>
<td>The user identity containing an account that has access to the desired domain or (none) when you want to use the CES service account.</td>
</tr>
<tr>
<td>Security Provider</td>
<td>(Optional) The security provider to map Email identities to another identity type.</td>
</tr>
</tbody>
</table>

4. Create an Exchange source. [more]

<table>
<thead>
<tr>
<th>Key parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>You must name your source.</td>
</tr>
</tbody>
</table>
### Key parameter | Value
--- | ---
Source Type | Exchange (WebServices)
Addresses | https://outlook.office365.com/
OwnerOnlySecurity (hidden parameter) | true
Active Directory Security Provider | Active Directory or a custom Active Directory security provider that you created for a specific domain.
Authentication | The user identity you created.

#### 9.27.6 Microsoft Exchange Configuration for the Connector

The topics in this section describe configuration to be made on the Microsoft Exchange server for the deployment of the Coveo connector.

#### 9.27.6.1 Creating a Microsoft Exchange Crawling Account

The Exchange connector needs an Exchange account to be able to access and index your Exchange content. The Exchange connector supports different Exchange deployment configurations. The requirements for the crawling account depend on the deployment configuration.

While you can use an existing account that meets the requirements, the best practice is to create an Exchange account dedicated to the Coveo connector. If you must occasionally or regularly change the account password, ensure to immediately also change the password in the CES user identity that holds the credentials to prevent source indexing update issues.

- Crawling account for an Exchange On-Premises Server
  
  For an Exchange On-Premises server, the crawling account must have full read access to all the Exchange content that you want to index (see "Setting up a Full Read Microsoft Exchange Account" on page 1185).

- Crawling account for an Exchange hybrid deployment
  
  In the context of an Exchange hybrid deployment, you must use two sources, one for the local content hosted on the Exchange On-Premises Server 2013, and one for the remote archives hosted on Exchange Online (see "About the Support for Exchange Server 2013 Hybrid Deployments" on page 1175). You can however use the same crawling account for both sources.

  When crawling remote archives, the Exchange connector must establish multiple secure connections with different services listed in the following table. In a best case scenario, a single user identity can be used to access all these services. As you can see from the table, the only identity format that is common to all required services is the UPN/SMTP format (ces_crawling@mycompany.com) that must therefore be used when creating the user identity to be associated with the source for the remote part of an hybrid deployment.
### Service Identity | Identity format
--- | ---
Exchange Online EWS | Exchange online user (Synced with AD or in cloud) with the ApplicationImpersonation role (see "Enabling Impersonation in Microsoft Exchange Online" on page 1193)
| ces_crawling@mycompany.com or ces_crawling@mycompany.onmicrosoft.com
Exchange On-Premises PowerShell | Exchange On-Premises Server administrator
| ces_crawling@mycompany.com or mycompany\ces_crawling
Active Directory | Any valid Active Directory account
| ces_crawling@mycompany.com or mycompany\ces_crawling

Note: When a user with all the above properties does not exist and cannot be created, you can use the PowerShellUserName and PowerShellPassword hidden parameters to create and specify an additional user identity on the source (see Modifying Hidden Microsoft Exchange Source Parameters).

- **CES 7.0.7814+ (August 2015)** Crawling account for an Exchange Online

  Depending on your setup:
  - When your users are cloud-based
    
    The crawling account can be the same Office 365 administrator account that you use to allow the connector access to the Exchange Online mailboxes of your Azure AD users (see "Authorizing the Coveo Connector to Access the Exchange Online Mailboxes of Your Azure AD Users" on page 1186).

    Note: The Office 365 account must have at least the following roles:
    - Exchange administrator
    - User management administrator

  - When your users are federated
    
    The crawling account must have full read access to all the Exchange content that you want to index (see "Setting up a Full Read Microsoft Exchange Account" on page 1185).

What's Next?

Create a CES user identity to hold the credentials of the Exchange account that you created for the Coveo connector exclusive use (see "Adding a User Identity" on page 420).
9.27.6.1.1 Setting up a Full Read Microsoft Exchange Account

You need to set up a special account in the Microsoft Exchange Server to be able to crawl multiple mailboxes using a single source. This account must have read access on all the mailboxes and all the public folders that you want to index.

Note: The best practice is to create a dedicated account for the Coveo connector. Coveo recommends using an account which has a password that never expires to avoid crawling problems. Otherwise, you must update the password in the user identity after each password change.

To set up a full read Microsoft Exchange account

1. For a Microsoft Exchange Server 2003 installation, refer to the following Microsoft article for information on how to set up such an account: How to assign service account access to all mailboxes in Exchange Server 2003

2. For Microsoft Exchange Server Online (only with federated users), 2013 (On-Premises and hybrid), 2010, and 2007 installations, use one of the following methods:

Note: CES 7.0.7814+ (August 2015) Support for Microsoft Exchange Online.

- Method 1 - Recommended

  Note: This method grants read permissions to the crawling account for all existing mailboxes, but also automatically for all mailboxes that will be created in the future.


  b. Run the following command, and then note the value for the Identity parameter:

     Get-OrganizationConfig

  c. Run the following command:

     Add-ADPermission -user [crawling_account] -Identity [Identity] -AccessRights ReadProperty, GenericExecute -ExtendedRights "Receive-As"

     where you replace:

     ○ [crawling_account] by the name of your crawling account, or probably a best practice, by the name of a dedicated Active Directory group containing only your crawling account.

     ○ [Identity] by the value that you noted for the Identity parameter from the first command.

- Method 2 - Plan B

  Important: This Exchange Management Shell command applies the permissions to currently existing users. You must therefore repeat this procedure each time a new mailbox is added to Exchange to ensure that the crawling account gains access to the new mailbox content.

  It is therefore recommended to schedule to automatically execute the procedure at an appropriate time interval.
a. Ensure that the crawling account has an active mailbox on a Microsoft Exchange server.

To crawl a Microsoft Exchange 2013/2010 server, the active mailbox of the account must be on a Microsoft Exchange 2013/2010 server.


c. Type the following command to give sufficient rights to a user to crawl using WebDAV or WebServices, depending on your Exchange Server location:

   - For on-premises servers [Exchange 2013 (On-Premises and hybrid), 2010 and 2007]:
     
     ```
     get-mailbox -server ServerName -ResultSize Unlimited | Add-MailboxPermission -User 'mydomain\myuser' -AccessRights FullAccess
     ```
     
     where you replace:
     - `ServerName` by the name of your Exchange server
     - `domain\user` by the user that you want to use to crawl the Microsoft Exchange content.

   - For online servers:
     
     ```
     get-mailbox -ResultSize Unlimited | Add-MailboxPermission -User 'mydomain\myuser' -AccessRights FullAccess
     ```
     
     where you replace `domain\user` by the user that you want to use to crawl the Microsoft Exchange content.

What's Next?

For a Microsoft Exchange 2013 or 2010 server, configure the throttling policy to prevent crawling problems (see "Configuring the Throttling Policy for the Microsoft Exchange Account" on page 1190).

For other Microsoft Exchange servers, configure a CES user identity (see "Adding a User Identity" on page 420).

9.27.6.2 Authorizing the Coveo Connector to Access the Exchange Online Mailboxes of Your Azure AD Users

**CES 7.0.7814+ (August 2015)**

When you want to index Microsoft Exchange Online mailboxes of cloud-based users (listed using Azure AD), you must perform the OAuth 2.0 protocol of your choice to authorize the Coveo connector to access the mailboxes content.

**Note:** In Azure AD, users with an on-premises Exchange plan and users with an Exchange Online plan cannot be distinguished, meaning that it is currently not possible via a Microsoft API to ONLY list Exchange Online users/mailboxes. However, using the procedure outlines in this topic, the content of all Exchange Online mailboxes of your organization will be searchable and accessible by their owner. Moreover, during the indexing process, all local mailboxes, which are owned by on-premises Exchange users, are ignored.
The OAuth 2.0 protocol is a protocol used for granting access to external applications without exposing the user’s real credentials. For the connector to be able to connect to your Exchange Online users, it must acquire a client ID, a key, a Windows Azure AD Graph API endpoint, and an OAuth 2.0 token endpoint.

To authorize the connector to access the Exchange Online mailboxes of your Azure AD users

1. Log in to the Windows Azure management portal with an administrator account.
   - (When you do not have a Microsoft Azure account) Sign up to the Windows Azure management portal via the Office 365 admin center (see Sign up for an Azure Subscription with Your Office 365 Account).

2. In the Windows Azure management portal, in the navigation bar on the left, click Azure Active Directory.

3. In the [Directory tenant name] pane, in the navigation bar on the left, under Manage, click App registrations.

4. In the [Directory tenant name] - App registrations pane, in the action bar, click Endpoints.

5. In the Endpoints pane:
   - Take note of the following information that you will also need when configuring the source:
     - Microsoft Azure AD Graph API Endpoint
       - Note: The endpoint value is needed when you later configure the Microsoft Exchange source (see Configuring and Indexing Microsoft Exchange Sources for an Online Deployment).
     - OAuth 2.0 Token Endpoint
       - Note: The endpoint value is needed when you later configure the Microsoft Exchange source (see Configuring and Indexing Microsoft Exchange Sources for an Online Deployment).
   - Click the X icon.


7. In the Create pane that appears on the right, enter the information related to your application:
   - In the first box, enter a descriptive Name for the application.
   - Under Application type, click the drop-down list menu, and then select Web app / API.
   - In the Sign-on URL box, enter http://localhost.
     - Note: This parameter is not used by the application, but cannot be left empty.
   - At the bottom of the pane, click Create.

8. Back in the [Directory tenant name] - App registrations pane, click the application you just created.
9. In the Settings pane that appears, click Properties.

10. In the Properties pane:
   
   i. Take note of the Application ID.

   **Note:** The Application ID value is needed when you later configure the Microsoft Exchange source (see Configuring and Indexing Microsoft Exchange Sources for an Online Deployment).

   ii. Next to Multi-tenanted, ensure No is selected.

   iii. Click Save.

11. In the Settings pane, click Required permissions.

12. In the Required permissions pane, click Windows Azure Active Directory
In the Enable Access pane that appears:

a. Click the Application permissions check box.

b. Click the Read directory data checkbox, and clear the other checkboxes.

c. Click Save.

Back in the Required permissions pane, click Grant permissions, and then in the confirmation prompt click Yes.

In the Settings pane, click Keys.

In the Keys pane:

a. In the first box on the left, enter a Key description.

b. Click the Duration drop-down list menu, and then select Never expires.

c. Click Save.

d. Upon successful configuration, your key Value appears. Copy and store this value that you will need when configuring your Exchange source in a secure location.

**Important:** The key value is only displayed once and is not retrievable afterwards.

**Note:** The key value is needed when you later configure the Microsoft Exchange source (see Configuring and Indexing Microsoft Exchange Sources for an Online Deployment).

e. Click the X icon.
What's Next?

Configure your Microsoft Exchange source (see "Configuring and Indexing Microsoft Exchange Sources for an Online Deployment" on page 1215).

9.27.6.3 Configuring the Throttling Policy for the Microsoft Exchange Account

In Exchange 2010, Microsoft introduced the throttling policy feature that is also present in Exchange 2013 and Online. With this feature, Exchange tracks the resources that each user consumes and enforces connection bandwidth limits, as necessary.

The throttling restrictions however negatively impacts the performance of the Coveo crawler that inevitably increases the load on the Microsoft Exchange Server. The default throttling policy assigned to Exchange users is too restrictive for crawling operations, causing numerous errors and problems that drastically decrease performance and possibly prevent access to some content.

The following tables describe the effects of the Microsoft Exchange throttling parameters on the crawling depending on the Microsoft Exchange version.

- **Exchange 2013**

<table>
<thead>
<tr>
<th>Throttling parameter</th>
<th>Effect</th>
</tr>
</thead>
<tbody>
<tr>
<td>EWSMaxConcurrency</td>
<td>When the value of this parameter is too low, you can get an error/warnings similar to:</td>
</tr>
<tr>
<td>EwsMaxBurst</td>
<td>[url] could not be accessed by Web Services: The server cannot service this request right now. Try again later.</td>
</tr>
<tr>
<td>EwsRechargeRate</td>
<td>Defines the rate at which an EWS user budget is recharged (budget grows by) during the budget time. This value is related to the EwsMaxBurst parameter.</td>
</tr>
<tr>
<td>EwsCutoffBalance</td>
<td>Defines the resource consumption limits for EWS user before that user is completely blocked from performing operations on a specific component. When this situation occurs, you can get an error/warnings similar to:</td>
</tr>
<tr>
<td></td>
<td>[url] generated this error: The operation has timed out, WebException status: Timeout.</td>
</tr>
<tr>
<td>EWSFindCountLimit</td>
<td>When the value of this parameter is too low, you can get error/warnings similar to:</td>
</tr>
<tr>
<td></td>
<td>You have exceeded the maximum number of objects that can be returned for the find operation. Use paging to reduce the result size and try your request again.</td>
</tr>
<tr>
<td>EWSMaxSubscriptions</td>
<td>This parameter affects the callback service, which prevents it from getting as many subscriptions as it needs. The Subscribe operation fails with an error status, the ErrorExceededSubscriptionCount response code, and the message: You have exceeded the available subscriptions for your account. Remove unnecessary subscriptions and try your request again.</td>
</tr>
</tbody>
</table>

- **Exchange 2010**
<table>
<thead>
<tr>
<th>Throttling parameter</th>
<th>Effect</th>
</tr>
</thead>
<tbody>
<tr>
<td>EWSMaxConcurrency</td>
<td>When the value of this parameter is too low, you can get error/warnings similar to: [url] could not be accessed by Web Services: The server cannot service this request right now. Try again later.</td>
</tr>
<tr>
<td>EWSPercentTimeInAD</td>
<td></td>
</tr>
<tr>
<td>EWSPercentTimeInCAS</td>
<td>When the value of this parameter is too low, you can get error/warnings similar to: [url] generated this error: The operation has timed out, WebException status : Timeout</td>
</tr>
<tr>
<td>EWSPercentTimeInMailBoxRPC</td>
<td></td>
</tr>
<tr>
<td>EWSFindCountLimit</td>
<td>When the value of this parameter is too low, you can get error/warnings similar to: You have exceeded the maximum number of objects that can be returned for the find operation. Use paging to reduce the result size and try your request again.</td>
</tr>
<tr>
<td>EWSMaxSubscriptions</td>
<td>This parameter affects the callback service, which prevents it from getting as many subscriptions as it needs. The Subscribe operation fails with an error status, the ErrorExceededSubscriptionCount response code, and the message: You have exceeded the available subscriptions for your account. Remove unnecessary subscriptions and try your request again.</td>
</tr>
</tbody>
</table>

**Note:** For more information on the following aspects refer to the corresponding Microsoft document:

- How to manipulate the policies: Modifying Throttling Policies
- How to read IIS logs for policy usage: Exchange API-spotting

You need to configure the throttling policy to grant unlimited access to the Exchange Web Services for the user that the connector will use to crawl the Microsoft Exchange content.

To configure the throttling policy for the Microsoft Exchange account

1. Using an administrator account, connect to your Microsoft Exchange Server.
2. Open the Exchange Management Shell, and then:
   a. Type the following command to create a new throttling policy called CoveoCrawlingPolicy:
      ```
      New-ThrottlingPolicy -Name CoveoCrawlingPolicy -EWSMaxConcurrency Unlimited -EWSMaxBurst Unlimited -EWSRechargeRate Unlimited -EWSCutoffBalance Unlimited -EWSMaxSubscriptions Unlimited
      ```
Note: For the online part of an Exchange 2013 hybrid deployment and an Exchange Online deployment, the throttling policy cannot be configured. The Coveo connector will be slowed down but manages the throttling related errors.

- For Exchange 2010:

```
New-ThrottlingPolicy -Name CoveoCrawlingPolicy -EWSMaxConcurrency $null -EWSPercentTimeInAD $null -EWSFindCountLimit $null -EWSPercentTimeInMailboxRPC $null -EWSFastSearchTimeoutInSeconds $null -EWSMaxSubscriptions $null -EWSPercentTimeInCAS $null
```

b. Type the following command to retrieve this new throttling policy and assign it to a variable:

```
$b = Get-ThrottlingPolicy CoveoCrawlingPolicy
```

c. Type the following command to assign the throttling policy to the coveoUser:

```
Set-Mailbox -Identity coveoUser -ThrottlingPolicy $b
```

where you replace coveoUser by the username that you selected to crawl the Microsoft Exchange content.

Note: The Coveo user must have a mailbox.

What's Next?

When you want to index the content of Exchange 2010 public folders, ensure that your Exchange server is correctly configured to prevent public folder crawling issues (see "Preventing Microsoft Exchange Public Folder Crawling Issues" on page 1192).

Otherwise you are ready to configure a CES user identity (see "Adding a User Identity" on page 420).

9.27.6.4 Preventing Microsoft Exchange Public Folder Crawling Issues

The Coveo connector for Microsoft Exchange servers can crawl Exchange 2010 public folders, but you need to ensure that your Exchange server is correctly configured to prevent public folder crawling issues.

To prevent public folder crawling issues

1. Refer to the Microsoft article Change the Default Public Folder Database for a Mailbox Database to find out how to ensure that while the connector points at an Exchange 2010 client access server (CAS), Exchange, behind the scene, does not point to a public folder database that is not compatible with Exchange 2010 Web Services.

   When this is the case, you may encounter the following errors while crawling Exchange 2010 folders:

   - https://server2010/public/ could not be accessed by Web Services: The mailbox that was requested doesn't support the specified RequestServerVersion.

2. Refer to the Microsoft article Configure Public Folder Replication to find out how to ensure that the targeted
public folders are correctly replicated on the default Public Folder Database for the account used by the connector to crawl the Microsoft Exchange content.

When this is the case, you may encounter Not Found error messages.

9.27.6.5 Enabling Impersonation in Microsoft Exchange Online

The Coveo Exchange connector usually relies on the CES crawling identity to have full access permissions to all mailboxes and their corresponding archive to index content from an Exchange On-Premises Server.

In an Exchange hybrid deployment, full access permission does not allow the CES crawling identity to access remote archives through Exchange Online Web Services (EWS). Only user impersonation can grant the CES crawling identity access to each user's remote archives. In an information system, impersonation is a mechanism that enables an application such as Coveo Enterprise Search (CES) to perform tasks on behalf of a user.

Consequently, in an Exchange hybrid deployment, when you want to index remote archives hosted on Exchange Online, you must enable impersonation for the CES crawling identity in your Exchange Online organization.

In Microsoft Exchange Online, the impersonation rights are granted to a user through the Exchange ApplicationImpersonation built-in management role.

To add the ApplicationImpersonation role to the CES crawling identity in Exchange Online

1. Connect PowerShell to your Exchange Online organization (see Use Windows PowerShell in Exchange Online).

   **Note:**
   - Administrative rights are needed to run the New-ManagementRoleAssignment command.
   - Before running Import-PSSession $Session, you might need to run Set-ExecutionPolicy Unrestricted (see Using the Set-ExecutionPolicy Cmdlet).
   - More information on role addition (see Add a role to a user or USG).

2. In a PowerShell command-line connected to your Exchange Online organization, run the following command, where you replace CES_crawler@mycompany.com by the user identity used by your source:

   PS> New-ManagementRoleAssignment -Role "ApplicationImpersonation" -User CES_crawler@mycompany.com

3. Validate the access to the Remote Archives on the Exchange Online server:
   a. Get the latest version of Microsoft EWSEditor.
   b. Create a new Exchange Service (File > New Exchange Service) using these parameters:
### Name | Value
--- | ---
Autodiscover - Exchange Version | Exchange2013
Credentials - User Name | CES crawling identity in UPN/SMTP format
Credentials - Password | Password of the CES crawling identity
Impersonation - Id Type | SmtpAddress
Impersonation - Id | SMTP address of one of the user with a Remote Archive to index

### 9.27.7 CES Configuration for the Microsoft Exchange Connector

The topics in this section describe configuration to be made on the Coveo server for the deployment of the Microsoft Exchange connector.

### 9.27.7.1 Configuring a Microsoft Exchange Security Provider

The Coveo connector needs a security provider to be able to get the permissions for each Microsoft Exchange item, and therefore fully support the Microsoft Exchange security model. This means that, in a Coveo search interface, a user searching for Microsoft Exchange content only sees the content to which he has access in Microsoft Exchange.

**Note:** You can get familiar with how Coveo components deal with permissions on documents both at indexing and query time.

To configure a Microsoft Exchange security provider:

1. On the Coveo server, access the Administration Tool.
2. Select **Configuration > Security**.
3. In the **Security** page, in the navigation panel on the left, click **Security Providers**.
4. In the **Security Providers** page, click **Add** to create a new security provider.
5. In the **Modify Security Provider** page:
a. In the Name box, enter a name to identify this security provider.

**Examples:**

- Microsoft Exchange On-Premises Security Provider
- Microsoft Exchange Hybrid Security Provider

b. In the Security Provider Type drop-down list:

   - On a 32-bit server, select Exchange (x86).
   - On a 64-bit server, select Exchange (x64).

c. In the User Identity section:

   i. In the drop-down list, select the user identity that you created previously for your Exchange On-Premises server or for your Exchange hybrid deployment sources.

   The security provider uses this identity to expand Exchange permissions. Ensure that the user has access to the Active Directory where Exchange users are defined, otherwise the document
permissions will not be resolved and users authenticated in a Coveo search interface will not be able to see their emails in search results.

When no identity is entered, by default the security provider takes the user which runs the CES service. A CES service user may not have access to Active Directory when it is the Local System account or a cross-domain user.

**Note:** You can select (none) in the **User Identity** drop-down list in which case the security provider automatically takes the user identity selected on the source to which it is associated. When you do so, ensure the source user identity can resolve security groups.

ii. When needed, click **Add, Edit, or Manage user identities** respectively to create, modify, or manage user identities.

d. In the **LDAP Search Root** box, enter the Lightweight Directory Access Protocol (LDAP) string to specify to the security provider where to start looking in Active Directory. When this parameter is not specified, the security provider looks at the root of Active Directory, which can be extremely large. By specifying a value, you can refine the search (see "What Are LDAP Searches?" on page 1230).

**Example:** To search only within the organizational unit (OU) `companynameOU` within the domain `corp.companyname.com`, enter:

```
LDAP://OU=companynameOU, DC=corp, DC=companyname, DC=com
```

e. In the **Active Directory Security Provider** drop-down list:

i. Select the appropriate security provider that this security provider uses to resolve and expand the groups.

   CES comes with an Active Directory security provider that you can configure to connect to the default domain. When you environment contains more than one domain, you can select an Active Directory security provider that you created for other domains.

ii. When an appropriate security provider is missing, click **Add, Edit, or Manage security providers** respectively to create, modify, or manage security providers.

f. **CES 7.0.6767+ (June 2014)** (Optional - For Exchange Online deployment only) In the **Exchange Online PowerShell Endpoint** box, enter the PowerShell endpoint to retrieve mailboxes from Microsoft Exchange.

**Example:** https://outlook.office365.com/powershell-liveid

**Note:** **CES 7.0.7814+ (August 2015)** It is rather recommended to use the Azure AD Graph API to list the Exchange Online mailboxes (see "Configuring and Indexing Microsoft Exchange Sources for an Online Deployment" on page 1215).

g. **CES 7.0.7022+ (September 2014)** (Optional - For Exchange Online deployment only) In the **Exchange Online Security Provider** drop-down list, select the security provider used to resolve Exchange Online cloud users.
h. In the Parameters section, in rare cases the Coveo Support could instruct you to click Add Parameters to specify other security provider parameter names and values that could help to troubleshoot security provider issues.

i. Leave the Allow Complex Identities option cleared as it does not apply to this type of security provider.

j. Click Apply Changes.

What's Next?

Configure and index a Microsoft Exchange source:

- When indexing only an Exchange On-Premises Server, see "Configuring and Indexing a Microsoft Exchange Source for an On-Premises Deployment" on page 1197.

- When indexing an Exchange Server 2013 hybrid deployment, see "Configuring and Indexing Microsoft Exchange Sources for a Hybrid Deployment" on page 1207.

9.27.7.2 Configuring and Indexing a Microsoft Exchange Source for an On-Premises Deployment

A source defines a set of configuration parameters for a given Microsoft Exchange Server deployment. This procedure describes how to create a source for an Exchange On-Premises Server deployment.

Note: For an Exchange 2013 hybrid deployment, you must create separate Exchange sources for the local and remote archives parts (see "Configuring and Indexing Microsoft Exchange Sources for a Hybrid Deployment" on page 1207).

Important:

- With Exchange Server 2013, to prevent having to build the source more than once, before building the source, configure the Exchange2013ViewModelValue hidden parameter to ensure that the OWA clickable URIs will be valid in search results (see Modifying Hidden Microsoft Exchange Source Parameters).

- In the out-of-the-box search interfaces preferences, end-users can clear the Open emails with Microsoft Outlook option to open email messages in Outlook Web App (OWA) rather than in Outlook when clicking an email search result.

To configure and index a Microsoft Exchange source

1. On the Coveo server, access the Administration Tool.

2. Select Index > Sources and Collections.

3. In the Collections section:

   a. Select an existing collection in which you want to add the new source.

   OR
b. Click **Add** to create a new collection.

4. In the **Sources** section, click **Add**.

The **Add Source** page that appears is organized in three sections.

5. In the **General Settings** section of the **Add Source** page:

   a. Enter the appropriate value for the following required parameters:

   **Name**
   
Enter a source name of your choice that represents the scope of the source.
   
   **Examples:** Microsoft Exchange Server

   **Source Type**
   
The connector used by this source. In this case, select **Exchange (WebServices)**.

   Select **Exchange (WebDAV)** only for Exchange 2003 or Exchange 2007 with Exchange 2003 compatibility mode (see “Choosing to Connect to Microsoft Exchange Using Web Services or WebDAV” on page 1204).

   **Note:** If you do not see **Exchange (WebServices)** or **Exchange (WebDAV)** in the **Source Type** list, your environment does not meet the requirements (see “Microsoft Exchange Connector Requirements” on page 1178).
Addresses

List of starting points for the connector. The connector supports both secured https and unsecured http servers.

Enter one address per line in one of the following forms:

- https://servername/exchange
- https://servername/exchange/mailboxname
- https://servername/public

Examples:

- To index all Microsoft Exchange mailboxes, enter a single URL that stops at the mailboxes root:
  
  https://owa.companyname.com/exchange

- To index all public folders, enter a URL that stops at the public folders root:
  
  https://owa.companyname.com/public

Note: Entering a specific server name will not restrict the crawled mailboxes to those located on that server (see "What Are LDAP Searches?" on page 1230).

Tip: You can create a source that only indexes Microsoft Exchange 2010 mailbox archives, pointing the connector directly to mailbox archives and skipping normal mailboxes using the http://server/exchange/onlinearchivename address pattern, where you replace onlinearchivename by the value found in the Active Directory field msExchArchiveName. You also need to ensure that the IndexArchives hidden parameter is set to true for this source and to false for the other Exchange source (see "IndexArchive (Boolean)" on page 1225).

Refresh Schedule

Time interval at which the index is automatically refreshed to keep the index content up-to-date. By default, the Every day option instructs CES to refresh the source everyday at 12 AM.

Note: You can create new or modify existing source refresh schedules.

b. Review the value for the following parameters that often do not need to be modified:

Rating

Change this value only when you want to globally change the rating associated with all items in this source relative to the rating to other sources.

Example: If this source was for Exchange archives only, you may want to set this parameter to Low, so that in the search interface, results from this source appear lower in the search results compared to those from other sources.

Document Types

If you defined custom document type sets, ensure to select the most appropriate for this source.
Active Languages

If you defined custom active language sets, ensure to select the most appropriate for this source.

Fields

If you defined custom field sets, ensure to select the most appropriate for this source.

6. In the **Specific Connector Parameters & Options** section of the **Add Source** page, review if you need to change the parameter default values:

![Specific Connector Parameters & Options](image)

**Max Number of Retries**

Number of reconnection attempts performed when the Exchange server fails to reply to a request.

**Retry Delay**

Delay between reconnection attempts in seconds.

**Exchange Folder**

Name of the folder hosting all the mailboxes. The default value is exchange. It corresponds to the segment of the URI that is after the server name and points to the mailboxes https://servername/exchange/.

**Use Form Authentication**

Whether to use forms-based authentication or not. The check box is cleared by default.

Select the check box when forms-based authentication is enabled on the Microsoft Exchange server. The connector supports two forms-based authentication types:
- Standard Microsoft Exchange forms-based authentication.
- ISA server forms-based authentication. When an ISA filter is put in front of the Microsoft Exchange OWA server.

**Index Exchange Security**

Whether to index the permissions specified in Microsoft Outlook or not. The check box is selected by default.

Clear this check box when you want to prevent the Coveo connector from indexing user defined permissions, in which case, only Active Directory permissions are used.

**Callback Service Url**

Optional parameter indicating the location of the Exchange Callback Service that enhances the incremental refresh performance on Microsoft Exchange 2007, 2010, and 2013 (On-Premises and hybrid) (see "Fine-Tuning the Exchange Callback Service" on page 1204).

The default value (http://localhost:8181/) is appropriate when the Exchange Callback Service runs on the same machine as CES. When the service runs on another computer, replace localhost by the Exchange server machine name. Change the port when the service does not use the default port (8181). Leave the parameter empty to disable the service.

**Public Folder**

Name of the public folder. The default value is public. It corresponds to the segment of the URI that is after the server name and that points to the public folders https://servername/public/.

**Index Junk E-mails**

Whether to index junk emails or not. Junk emails are indexed by default.

**Skip 3rd Party Archived Items**

Whether to skip indexing of items archived by an external archiving system, such as Symantec Enterprise Vault. This parameter is useful to make the Microsoft Exchange connector ignore email stubs left behind by an external archiving system. The check box is selected by default.

**Notes:**

- Do not confuse the Skip 3rd Party Archived Items with the IndexArchive hidden parameter, which controls whether Exchange archive mailboxes should be indexed (see Modifying Hidden Microsoft Exchange Source Parameters).

- CES 7.0.6767– (June 2014) The parameter is named Skip Archived Items.

**Parameters**

Click Add Parameter when you want to show and configure advanced hidden source parameters (see "Modifying Hidden Microsoft Exchange Source Parameters" on page 1222).

In the Option section:
Index Subfolders

Check to index all subfolders below the specified starting addresses. Selected by default.

Index the document’s metadata

When selected, CES indexes all the document metadata, even metadata that are not associated with a field. The orphan metadata are added to the body of the document so that they can be searched using free text queries.

When cleared (default), only the values of system and custom fields that have the Free Text Queries attribute selected will be searchable without using a field query.

Example: A document has two metadata:

- LastEditedBy containing the value Hector Smith
- Department containing the value RH

In CES, the custom field CorpDepartment is bound to the metadata Department and its Free Text Queries attribute is selected.

When the Index the document’s metadata option is cleared, searching for RH returns the document because a field is indexing this value. Searching for hector does not return the document because no field is indexing this value.

When the Index the document’s metadata option is selected, searching for hector also returns the document because CES indexed orphan metadata.

Generate a cached HTML version of indexed documents

When you select this check box (recommended), at indexing time, CES creates HTML versions of indexed documents. In the search interfaces, users can then more rapidly review the content by clicking the Quick View link rather than opening the original document with the original application. Consider clearing this check box only if you do not want to use Quick View links or to save resources when building the source.

Open results with cached version

Leave this check box cleared (recommended) so that in the search interfaces, the main search result link opens the original document with the original application. Consider selecting this check box only when you do not want users to be able to open the original document but only see the HTML version of the document as a Quick View. In this case, you must also select Generate a cached HTML version of indexed documents.

7. In the Security section of the Add Source page:
a. In the **Active Directory Security Provider** drop-down list, select **Active Directory** or a custom Active Directory security provider that you created for a specific domain.

b. In the **Exchange Security Provider** drop-down list, select the security provider that you created for this source (see "Configuring a Microsoft Exchange Security Provider" on page 1194).

c. In the **Authentication** drop-down list, select the user identity that you created for the Microsoft Exchange system.

d. Click **Save and Start** to save the source configuration and start indexing this source.

8. **Validate** that the source building process is executed without errors:

   - In the navigation panel on the left, click **Status**, and then validate that the indexing proceeds without errors.

   OR

   - Open the CES Console to monitor the source building activities.

**Note:** If you get a **PowerShellException** like the following, on the Coveo Master server, set Windows PowerShell execution policy to the **RemoteSigned** restriction to allow the connector script to run (see the Microsoft TechNet document: Using the **Set-ExecutionPolicy** Cmdlet).

---

Exchange (WebServices) Error: Error while listing mailboxes.
----> Coveo.Connectors.Utilities.PowerShell.PowerShellException: Error while evaluating PowerShell script. ----> System.Management.Automation.CmdletInvocationException: There were errors in loading the format data file:
... Microsoft.PowerShell, , C:\Temp\...ps1xml : File skipped because of the following validation exception: File C:\Temp\...ps1xml cannot be loaded because the execution of scripts is disabled on this system. Please see "get-help about_signing" for more details.

---

**What's Next?**

Set an incremental refresh schedule for your source.
Consider modifying advanced source parameters (see "Modifying Hidden Microsoft Exchange Source Parameters" on page 1222).

9.27.7.2.1 Choosing to Connect to Microsoft Exchange Using Web Services or WebDAV

The Coveo connector can connect to Microsoft Exchange servers using either the Web Services or WebDAV method. When you create a Microsoft Exchange source, two source types are available:

- Exchange (WebServices)
- Exchange (WebDAV)

The following table indicates which options are supported by which version of Microsoft Exchange.

<table>
<thead>
<tr>
<th>Microsoft Exchange Version</th>
<th>Exchange (WebServices)</th>
<th>Exchange (WebDAV)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Exchange 2013 hybrid deployments (remote part)</td>
<td>Supported</td>
<td>Not supported</td>
</tr>
<tr>
<td>Exchange 2013</td>
<td>Supported</td>
<td>Not supported</td>
</tr>
<tr>
<td>Exchange 2010</td>
<td>Supported</td>
<td>Not supported</td>
</tr>
<tr>
<td>Exchange 2007</td>
<td>Supported</td>
<td>Supported (when the Exchange 2003 Compatibility mode is installed)</td>
</tr>
<tr>
<td>Exchange 2003</td>
<td>Not supported</td>
<td>Supported</td>
</tr>
</tbody>
</table>

You should choose the Exchange (WebDAV) option only when indexing an Exchange 2003 server. For Exchange 2007 setups, it is recommended to use the WebServices option as it offers better performances and is simpler to configure.

**Note:** Once a source is created, you cannot change the source type (WebDAV or WebServices). You must then create a new source using the other source type.

When you choose WebDAV, be aware that the WebDAV protocol is prohibited by default in IIS. You must therefore enable WebDAV in IIS.

What's Next?

Configure and index the Microsoft Exchange source (see "Configuring and Indexing a Microsoft Exchange Source for an On-Premises Deployment" on page 1197).

9.27.7.2.2 Fine-Tuning the Exchange Callback Service

For Microsoft Exchange Server 2007, 2010 and 2013 (On-Premises and hybrid), the Coveo Exchange (WebServices) connector uses Microsoft Exchange callback service API to request notifications from Exchange when content is modified within a monitored mailbox. With this information, the connector can immediately update the good folders and items on the next incremental refresh run, instead of polling for every folder in every mailbox.
This ability drastically improves incremental refresh performances and reduces bandwidth usage. The CES installer deploys the callback service that starts when an Exchange WebServices connector requests it. By default, a new Exchange WebServices source is ready to use the Exchange Callback Service.

The **Callback Service Url** source parameter indicates the location of the Exchange Callback Service (see "Configuring and Indexing a Microsoft Exchange Source for an On-Premises Deployment" on page 1197).

### Notes: CES 7.0.8047+ (December 2015) (For Exchange Online only)

- Due to an Exchange Web Services limitation (which limits the number of online mailbox subscriptions to approximately 20), the callback service is disabled by default in the following three cases (see Exchange Online Throttling and Limits FAQ):
  - The starting addresses contain more than one Exchange Online address.
  - One of the starting addresses points to an Exchange Online folder.
    ```
    Example: https://outlook.office365.com/owa
    ```
  - One of the starting addresses points to an Exchange Online public folder.
    ```
    Example: https://outlook.office365.com/public
    ```
- When the callback service is disabled, the following message is shown in the CES Console:
  "Targeting multiple Exchange Online mailboxes. The Notification Callback Service will not be used because of Exchange Online subscription limit of 20 mailboxes. Use the parameter 'UseCallbackServiceForMultipleExchangeOnlineStartingItems' to override this behavior."
- If you still want to use the callback service to receive change notifications during incremental refreshes, have in mind that it will only work for 20 (or less) mailboxes or public folders. When you try to subscribe to more mailboxes/public folders, you get the following error message:
  ```
  Folder error: https://outlook.office365.com/public/[path]
  You have exceeded the available subscriptions for your account.
  Remove unnecessary subscriptions and try your request again.
  ```

### Important: Ensure to open the port 8181 in the firewall. The Exchange Server has to connect to the Exchange Callback Service to send notifications.

The Exchange Callback Service requires that a user identity is defined on the source to work.

When an Exchange WebServices source starts, a message appears in the CES log to specify whether the Exchange Callback Service is used or not, either because it is not configured correctly or cannot be started.

<table>
<thead>
<tr>
<th>Callback service state</th>
<th>Message in CES log when an Exchange (WebServices) source starts</th>
</tr>
</thead>
<tbody>
<tr>
<td>Used</td>
<td>[SourceName] - Using Push Notifications.</td>
</tr>
</tbody>
</table>
The Exchange Callback Service is configured to run correctly in most cases using default parameter values. You can however manually configure advanced parameters in the Exchange Callback Service configuration file to fine-tune out-of-the-box behaviors.

To fine-tune the Exchange Callback Service configuration file

1. Refer to the following list of available configuration file parameters to see if you need to change the default value of one or more of them.

   **LogFileLifeTime**
   
   Duration before a log file is automatically deleted by the service. Default is 30 days.

   **LogMaxSize**
   
   Maximum size before splitting a log file. Default is 10 MB (10485760 bytes).

   **MaxConnections**
   
   Maximum number of concurrent connections that the service can create when calling the Exchange WebServices. Default is 4 connections.

   **ShowAllCounters**
   
   Displays the usage statistics about the service in the CES console and logs before each incremental refresh run. Default is false.

   **DataFilePath**
   
   Location of the data files used by the service. By default, data files are located in the [Index_Path]\Index\Crawlers\ExchangeCallbackService folder.

   **LogFilePath**
   
   Location of the log files created by the service. By default, log files are saved in the same folder as the other CES log files ([Index_Path]\Log).

   **SubscriptionTimeout**
   
   Duration before an Exchange subscription is considered invalid. This value should not be changed unless there are issues using the default value. Default is 30 minutes. Maximum allowed is 1440 minutes.

   **HostName**
   
   Host name used internally to build the web service URL. Changing this value affects directly the Callback Service Url parameter that is set on an Exchange source. Default is the computer name.
PortNumber

Port number used internally to build the web service URL. Changing this value affects directly the Callback Service URL parameter that is set on an Exchange source. Default is 8181.

ReaderQuotas [CES 7.0.6607+ (April 2014)]

Default limits for the complexity of received messages (see XElementReaderQuotas Class). May need to be increased when recommended by Coveo Support to ensure proper communication from Exchange to the Callback service.

The default and recommended values are:

```xml
<readerQuotas
    maxDepth="2147483647"
    maxStringContentLength="2147483647"
    maxArrayLength="2147483647"
    maxBytesPerRead="2147483647"
    maxNameTableCharCount="2147483647"
/>
```

2. Using an administrator account, connect to the Coveo Master server.

3. Browse to the CES bin folder ([CES_Path]\Bin).

4. Using a text editor:
   a. Open the CESExchangeCallbackService.exe.config file.
   b. Under <configuration> in the content of the file, locate the <appSettings> section.
   c. Add one custom parameter per line under <appSettings> using the following format:

   ```xml
   <add key="parameter_name" value="value"/>
   ```
   d. Save the file.

**Example:** To specify a maximum number of connections equal to 6, add line 4 as shown in the following file excerpt.

```xml
<configuration>
    <appSettings>
        <add key="MaxConnections" value="6"/>
    ...
</appSettings>
</configuration>
```

9.27.7.3 Configuring and Indexing Microsoft Exchange Sources for a Hybrid Deployment

The Coveo connector supports indexing a Microsoft Exchange Server 2013 hybrid deployment where most of the content to index resides on an Exchange On-Premises Server 2013, and remote archives reside in Microsoft Exchange Online (see "About the Support for Exchange Server 2013 Hybrid Deployments" on page 1175).
Notes:

- CES 7.0.6684+ (May 2014) Indexing remote archives in the context of an Exchange Server 2013 hybrid deployment support.

- Do not use the procedure in this topic when you want to configure a source for Exchange content that fully resides on an Exchange On-Premises Server, rather see "Configuring and Indexing a Microsoft Exchange Source for an On-Premises Deployment" on page 1197.

A source defines a set of configuration parameters for a specific Microsoft Exchange Server. For an Exchange 2013 hybrid deployment, you must create two sources, respectively for the Exchange On-Premises Server (local) and the Microsoft Exchange Online (remote archives) parts.

**Important:**

- To prevent having to build the source more than once, before building the source, configure the Exchange2013ViewModelValue hidden parameter to ensure that the OWA clickable URIs will be valid in search results (see Modifying Hidden Microsoft Exchange Source Parameters).

- In the out-of-the-box search interfaces preferences, end-users can clear the Open emails with Microsoft Outlook option to open email messages in Outlook Web App (OWA) rather than in Outlook when clicking an email search result.

To configure and index Microsoft Exchange sources for a hybrid deployment

1. On the Coveo server, access the Administration Tool.

2. Select Index > Sources and Collections.

3. In the Collections section:
   a. Select an existing collection in which you want to add the new source.

   OR

   b. Click Add to create a new collection.

   **Note:** For each of the sources required in your hybrid deployment, repeat the following steps.

4. In the Sources section, click Add.

   The Add Source page that appears is organized in three sections.

5. In the General Settings section of the Add Source page:
a. Enter the appropriate value for the following required parameters:

**Name**

Enter a source name of your choice that represents the scope of the source.

**Examples:**
- For a hybrid local part: Microsoft Exchange hybrid (Local)
- For remote archives: Microsoft Exchange hybrid (Remote Archives)

**Source Type**

The connector used by this source. For an Exchange hybrid case, select Exchange (WebServices).

**Note:** If you do not see Exchange (WebServices) in the Source Type list, your environment does not meet the requirements (see "Microsoft Exchange Connector Requirements" on page 1178).

**Addresses**

List of starting points for the connector, typically one address. When you specify more than one address, you must ensure that all other parameter values apply to all specified starting addresses. The connector supports both secured https and unsecured http servers.
For the local Exchange On-Premises Server part:

**Examples:**
- To index all Microsoft Exchange mailboxes, enter a single URL that stops at the mailboxes root:
  
  https://owa.companyname.com/exchange

- To index all public folders, enter a URL that stops at the public folders root:
  
  https://owa.companyname.com/public

For the remote archives part on Microsoft Exchange Online, the address is always the same:

https://outlook.office365.com/

**Schedule**

Time interval at which the index is automatically refreshed to keep the index content up-to-date. By default, the **Every day** option instructs CES to refresh the source everyday at 12 AM.

**Note:** You can create new or modify existing source refresh schedules.

b. Review the value for the following parameters that often do not need to be modified:

**Rating**

Change this value only when you want to globally change the rating associated with all items in this source relative to the rating to other sources.

**Example:** If this source was for a local or remote Exchange archive, you may want to set this parameter to **Low**, so that in the search interface, results from this source appear lower in the search results compared to those from other sources.

**Document Types**

If you defined custom document type sets, ensure to select the most appropriate for this source.

**Active Languages**

If you defined custom active language sets, ensure to select the most appropriate for this source.

**Fields**

If you defined custom field sets, ensure to select the most appropriate for this source.

6. In the **Specific Connector Parameters & Options** section of the **Add Source** page, review if you need to change the parameter default values:
Max Number of Retries

Number of reconnection attempts performed when the Exchange server fails to reply to a request.

Retry Delay

Delay between reconnection attempts in seconds.

Exchange Folder

Name of the folder hosting all the mailboxes. The default value is `exchange`. It corresponds to the segment of the URI that is after the server name and points to the mailboxes `https://ExchangeServer/exchange/`.

Use Form Authentication

Whether to use forms-based authentication or not. The check box is cleared by default.

Select the check box when forms-based authentication is enabled on the Microsoft Exchange Server. The connector supports two forms-based authentication types:

- Standard Microsoft Exchange forms-based authentication.
- ISA server forms-based authentication. When an ISA filter is put in front of the Microsoft Exchange OWA server.
Index Exchange Security

Whether to index the permissions specified in Microsoft Outlook or not. The check box is selected by default.

Clear this check box when you want to prevent the Coveo connector from indexing user defined permissions, in which case, only Active Directory permissions are used.

Callback Service Url

Optional parameter indicating the location of the Exchange Callback Service that enhances the incremental refresh performance on Microsoft Exchange 2007, 2010, and 2013 (On-Premises and hybrid) (see "Fine-Tuning the Exchange Callback Service" on page 1204).

The default value (http://localhost:8181/) is appropriate when the Exchange Callback Service runs on the same machine as CES. When the service runs on another computer, replace localhost by the Exchange server machine name. Change the port when the service does not use the default port (8181). Leave the parameter empty to disable the service.

Public Folder

Name of the public folder. The default value is public. It corresponds to the segment of the URI that is after the server name and that points to the public folders https://ExchangeServer/public/.

Index Junk Emails

Whether to index junk emails or not. Junk emails are indexed by default.

Skip 3rd Party Archived Items

Whether to skip indexing of items archived by an external archiving system, such as Symantec Enterprise Vault. This parameter is useful to make the Microsoft Exchange connector ignore email stubs left behind by an external archiving system. The check box is selected by default.

Notes:

- Do not confuse the Skip 3rd Party Archived Items with the IndexArchive hidden parameter, which controls whether Exchange archive mailboxes should be indexed (see Modifying Hidden Microsoft Exchange Source Parameters).
- CES 7.0.6830–(July 2014) The parameter name was Skip Archived Items.

Parameters

Click Add Parameter when you want to show and configure advanced hidden source parameters (see "Modifying Hidden Microsoft Exchange Source Parameters" on page 1222).

For the remote archives source, add the hidden parameters and values listed in the following table.
In the Option section:

**Index Subfolders**

Check to index all subfolders below the specified starting addresses. Selected by default.

**Index the document's metadata**

When selected, CES indexes all the document metadata, even metadata that are not associated with a field. The orphan metadata are added to the body of the document so that they can be searched using free text queries.

When cleared (default), only the values of system and custom fields that have the Free Text Queries attribute selected will be searchable without using a field query.

**Example:** A document has two metadata:
- `LastEditedBy` containing the value Hector Smith
- `Department` containing the value RH

In CES, the custom field `CorpDepartment` is bound to the metadata `Department` and its Free Text Queries attribute is selected.

When the **Index the document's metadata** option is cleared, searching for RH returns the document because a field is indexing this value. Searching for hector does not return the document because no field is indexing this value.

When the **Index the document's metadata** option is selected, searching for hector also returns the document because CES indexed orphan metadata.

**Generate a cached HTML version of indexed documents**

When you select this check box (recommended), at indexing time, CES creates HTML versions of indexed documents. In the search interfaces, users can then more rapidly review the content by clicking the Quick View link rather than opening the original document with the original application. Consider clearing this check box only if you do not want to use Quick View links or to save resources when building the source.

**Open results with cached version**

Leave this check box cleared (recommended) so that in the search interfaces, the main search result link
opens the original document with the original application. Consider selecting this check box only when you do not want users to be able to open the original document but only see the HTML version of the document as a Quick View. In this case, you must also select **Generate a cached HTML version of indexed documents**.

7. In the **Security** section of the **Add Source** page:

![Security section of Add Source page]

   a. In the **Active Directory Security Provider** drop-down list, select **Active Directory** or a custom Active Directory security provider that you created for a specific domain.

   b. In the **Exchange Security Provider** drop-down list, select the security provider that you created for this source (see "Configuring a Microsoft Exchange Security Provider" on page 1194).

   c. In the **Authentication** drop-down list, select the user identity that you created for the Microsoft Exchange system.

   d. Click **Save and Start** to save the source configuration and start indexing this source.

8. Validate that the source building process is executed without errors:

   - In the navigation panel on the left, click **Status**, and then validate that the indexing proceeds without errors.

   OR

   - Open the CES Console to monitor the source building activities.
Note: If you get a PowerShellException like the following, on the Coveo Master server, set Windows PowerShell execution policy to the RemoteSigned restriction to allow the connector script to run (see the Microsoft TechNet document: Using the Set-ExecutionPolicy Cmdlet).

```
Exchange (WebServices) Error: Error while listing mailboxes.
  ---> Coveo.Connectors.Utilities.PowerShell.PowerShellException: Error while evaluating PowerShell script. ---> System.Management.Automation.CmdletInvocationException: There were errors in loading the format data file:
... Microsoft.PowerShell, , C:\Temp\...ps1xml : File skipped because of the following validation exception: File C:\Temp\...ps1xml cannot be loaded because the execution of scripts is disabled on this system. Please see "get-help about_signing" for more details.
```

What's Next?

Set an incremental refresh schedule for your source.

Consider modifying advanced source parameters (see "Modifying Hidden Microsoft Exchange Source Parameters" on page 1222).

9.27.7.4 Configuring and Indexing Microsoft Exchange Sources for an Online Deployment

CES 7.0.7814+ (August 2015)

The Coveo connector supports indexing Microsoft Exchange Online mailboxes whether the mailbox owners are federated (listed in a local AD and synced or not in Azure AD) or cloud-based users (will be listed using Azure AD). The only requirement for an online mailbox to be indexed is that the mailbox owner can be found either in a local AD or using Azure AD.

Notes:

- In Azure AD, users with an on-premises Exchange plan and users with an Exchange Online plan cannot be distinguished, meaning that it is currently not possible via a Microsoft API to ONLY list Exchange Online users/mailboxes. However, using the procedure outlines in this topic, the content of all Exchange Online mailboxes of your organization will be searchable and accessible by their owner. Moreover, during the indexing process, all local mailboxes, which are owned by on-premises Exchange users, are ignored.

- Do not use the procedure in this topic when you want to configure a source for Exchange content that fully resides on an Exchange On-Premises Server, rather see "Configuring and Indexing a Microsoft Exchange Source for an On-Premises Deployment" on page 1197.

A source defines a set of configuration parameters for a specific Microsoft Exchange server.

To configure and index Microsoft Exchange sources for an online deployment

1. On the Coveo server, access the Administration Tool.
2. Select Index > Sources and Collections.
3. In the Collections section:
a. Select an existing collection in which you want to add the new source.

OR

b. Click **Add** to create a new collection.

4. In the **Sources** section, click **Add**.

The **Add Source** page that appears is organized in three sections.

5. In the **General Settings** section of the **Add Source** page:

   ![General Settings](image)

   a. Enter the appropriate value for the following required parameters:

   **Name**

   Enter a source name of your choice that represents the scope of the source.

   **Example:** Microsoft Exchange Online Mailboxes

   **Source Type**

   The connector used by this source. For an Exchange Online case, select **Exchange (WebServices)**.

   **Note:** If you do not see **Exchange (WebServices)** in the **Source Type** list, your environment does not meet the requirements (see "Microsoft Exchange Connector Requirements" on page 1178).

   **Addresses**

   List of starting points for the connector, typically one address. When you specify more than one
address, you must ensure that all other parameter values apply to all specified starting addresses. The connector supports both secured https and unsecured http servers.

For Microsoft Exchange Online, the address is always the same:

https://outlook.office365.com/

**Refresh Schedule**

Time interval at which the index is automatically refreshed to keep the index content up-to-date. By default, the *Every day* option instructs CES to refresh the source everyday at 12 AM.

**Note:** You can create new or modify existing source refresh schedules.

b. Review the value for the following parameters that often do not need to be modified:

**Rating**

Change this value only when you want to globally change the rating associated with all items in this source relative to the rating to other sources.

**Example:** If this source was for a local or remote Exchange archive, you may want to set this parameter to Low, so that in the search interface, results from this source appear lower in the search results compared to those from other sources.

**Document Types**

If you defined custom document type sets, ensure to select the most appropriate for this source.

**Active Languages**

If you defined custom active language sets, ensure to select the most appropriate for this source.

**Fields**

If you defined custom field sets, ensure to select the most appropriate for this source.

6. In the **Specific Connector Parameters & Options** section of the **Add Source** page, review if you need to change the parameter default values:
Max Number of Retries

Number of reconnection attempts performed when the Exchange server fails to reply to a request.

Retry Delay

Delay between reconnection attempts in seconds.

Exchange Folder

Name of the folder hosting all the mailboxes. The default value is `exchange`. It corresponds to the segment of the URI that is after the server name and points to the mailboxes


Use Form Authentication

Whether to use forms-based authentication. The check box is cleared by default.

Select the check box when forms-based authentication is enabled on the Microsoft Exchange Server. The connector supports two forms-based authentication types:

- Standard Microsoft Exchange forms-based authentication.
- ISA server forms-based authentication. When an ISA filter is put in front of the Microsoft Exchange OWA
server.

Index Exchange Security

Whether to index the permissions specified in Microsoft Outlook. The check box is cleared by default.

Select this check box when you want the Coveo connector to index user defined permissions as well as the Active Directory permissions.

Callback Service Url

Note: **CES 7.0.8047+ (December 2015)** Due to an Exchange Web Services limitation (which limits the number of online mailbox subscriptions to approximately 20), the callback service is no longer used by default (see Exchange Online Throttling and Limits FAQ).

If you still want to use the callback service to receive change notifications during incremental refreshes (by setting the `UseCallbackServiceForMultipleExchangeOnlineStartingItems hidden parameter to true`), have in mind that it will only work for 20 (or less) mailboxes or public folders (see Modifying Hidden Microsoft Exchange Source Parameters). When you try to subscribe to more mailboxes/public folders, you get the following error message:

Folder error: https://outlook.office365.com/public/[path]

You have exceeded the available subscriptions for your account.

Remove unnecessary subscriptions and try your request again.

(When you set the `UseCallbackServiceForMultipleExchangeOnlineStartingItems hidden parameter to true`) Parameter indicating the location of the Exchange Callback Service that enhances the incremental refresh performance when you have less than 20 mailboxes or public folder to index (see "Fine-Tuning the Exchange Callback Service" on page 1204).

The default value (http://localhost:8181/) is appropriate when the Exchange Callback Service runs on the same machine as CES. When the service runs on another computer, replace localhost by the Exchange server machine name. Change the port when the service does not use the default port (8181). Leave the parameter empty to disable the service.

Public Folder

Name of the public folder. The default value is public. It corresponds to the segment of the URI that is after the server name and that points to the public folders https://ExchangeServer/public/.

Index Junk Emails

Whether to index junk emails or not. Junk emails are indexed by default.

Skip 3rd Party Archived Items

Whether to skip indexing of items archived by an external archiving system, such as Symantec Enterprise Vault. This parameter is useful to make the Microsoft Exchange connector ignore email stubs left behind by an external archiving system. The check box is selected by default.
Note: Do not confuse the Skip 3rd Party Archived Items with the IndexArchive hidden parameter, which controls whether Exchange archive mailboxes should be indexed (see Modifying Hidden Microsoft Exchange Source Parameters).

Parameters

Click Add Parameter to show and change the value of the following required hidden source parameters (see "Modifying Hidden Microsoft Exchange Source Parameters" on page 1222):

Depending on your setup:

- When your users are cloud-based (Azure AD users):

<table>
<thead>
<tr>
<th>Parameter name</th>
<th>Parameter value</th>
</tr>
</thead>
<tbody>
<tr>
<td>AzureAdOAuth2TokenEndpoint</td>
<td>The endpoint used to obtain an access token using OAuth 2.0 (see Authorizing the Coveo Connector to Access the Exchange Online Mailboxes of Your Azure AD Users).</td>
</tr>
<tr>
<td>AzureAdGraphApiEndpoint</td>
<td>The endpoint used by the Azure AD Graph API to access directory data in the Windows Azure AD directory (see Authorizing the Coveo Connector to Access the Exchange Online Mailboxes of Your Azure AD Users).</td>
</tr>
<tr>
<td>AzureAdClientId</td>
<td>The Azure AD client ID you previously obtained (see Authorizing the Coveo Connector to Access the Exchange Online Mailboxes of Your Azure AD Users).</td>
</tr>
<tr>
<td>AzureAdClientKey</td>
<td>The Azure AD client key you previously obtained (see Authorizing the Coveo Connector to Access the Exchange Online Mailboxes of Your Azure AD Users).</td>
</tr>
<tr>
<td>OwnerOnlySecurity</td>
<td>true</td>
</tr>
</tbody>
</table>

- When your users are federated (local AD users):

<table>
<thead>
<tr>
<th>Parameter name</th>
<th>Parameter value</th>
</tr>
</thead>
<tbody>
<tr>
<td>OwnerOnlySecurity</td>
<td>true</td>
</tr>
</tbody>
</table>

In the Option section:

Index Subfolders

Check to index all subfolders below the specified starting addresses. Selected by default.

Index the document's metadata

When selected, CES indexes all the document metadata, even metadata that are not associated with a field. The orphan metadata are added to the body of the document so that they can be searched using free
text queries.

When cleared (default), only the values of system and custom fields that have the **Free Text Queries** attribute selected will be searchable without using a field query.

**Example:** A document has two metadata:
- `LastEditedBy` containing the value Hector Smith
- `Department` containing the value RH

In CES, the custom field `CorpDepartment` is bound to the metadata `Department` and its **Free Text Queries** attribute is selected.

When the **Index the document's metadata** option is cleared, searching for RH returns the document because a field is indexing this value. Searching for hector does not return the document because no field is indexing this value.

When the **Index the document's metadata** option is selected, searching for hector also returns the document because CES indexed orphan metadata.

**Generate a cached HTML version of indexed documents**

When you select this check box (recommended), at indexing time, CES creates HTML versions of indexed documents. In the search interfaces, users can then more rapidly review the content by clicking the Quick View link rather than opening the original document with the original application. Consider clearing this check box only if you do not want to use Quick View links or to save resources when building the source.

**Open results with cached version**

Leave this check box cleared (recommended) so that in the search interfaces, the main search result link opens the original document with the original application. Consider selecting this check box only when you do not want users to be able to open the original document but only see the HTML version of the document as a Quick View. In this case, you must also select **Generate a cached HTML version of indexed documents**.

7. In the **Security** section of the **Add Source** page:
a. In the **Active Directory Security Provider** drop-down list, depending on your setup:

- When your users are cloud-based (Azure AD users), select **(none)**.

  **Note:** When the Azure AD hidden parameters are specified on the source, this parameter becomes optional.

- When your users are federated (local AD users), select **Active Directory** or a custom Active Directory security provider that you created for a specific domain.

b. In the **Exchange Security Provider** drop-down list, depending on your setup:

- When your users are cloud-based (Azure AD users), select the security provider that you created for this source (see Microsoft Exchange Connector Deployment Overview).

- When your users are federated (local AD users), select **(none)**.

c. In the **Authentication** drop-down list, select the user identity that you created for Microsoft Exchange Online.

  **Note:** The user must be in an email format and NOT in the domain\username format.

  **Example:** ces_crawling@mycompany.onmicrosoft.com

d. Click **Save and Start** to save the source configuration and start indexing this source.

8. Validate that the source building process is executed without errors:

- In the navigation panel on the left, click **Status**, and then validate that the indexing proceeds without errors.

  **OR**

- Open the CES Console to monitor the source building activities.

What's Next?

Set an incremental refresh schedule for your source.

Consider modifying advanced source parameters (see "Modifying Hidden Microsoft Exchange Source Parameters" on page 1222).

9.27.7.5 Modifying Hidden Microsoft Exchange Source Parameters

The **Add Source** and **Source**: ... **General** pages of the Administration Tool present the parameters with which you can configure the connector for most Microsoft Exchange setups. More advanced and more rarely used parameters are hidden. You can choose to make one or more of these parameters appear in the **Add Source** and **Source**: ... **General** pages of the Administration Tool so that you can change their default value.

The following list describes the available advanced hidden parameters for Microsoft Exchange sources. The parameter type (integer, string...) appears between parentheses following the parameter name.

**UseAdCache (Boolean)** CES 7.0.8047+ (December 2015)

Whether an Active Directory mailbox cache is used to reduce the number of AD calls required when the crawler...
browses the Exchange Active Directory server. The default value is `false`. Change the value to `true` when you have issues with the load on the Exchange Active Directory server (which can be due to several incremental refreshes in a short period of time).

**Note:** The cache is only used during incremental refresh operations and filled when the source is rebuilding or refreshing.

`UseCallbackServiceForMultipleExchangeOnlineStartingItems (Boolean)`  
**CES 7.0.8047+ (December 2015)**

Whether the Notification Callback Service is activated. The default value is `false`. Consider changing this value to `true` when you have 20 (or less) Exchange Online mailboxes or public folders.

**Note:** Due to an Exchange Web Services limitation, the maximum number of online mailbox subscriptions is approximately 20 (see Exchange Online Throttling and Limits FAQ).

When you try to subscribe to more mailboxes/public folders, you get the following error message:

Folder error: https://outlook.office365.com/public/\[path\]

You have exceeded the available subscriptions for your account.

Remove unnecessary subscriptions and try your request again.

**CES 7.0.7814+ (August 2015)**

List of required hidden parameters when indexing Exchange Online mailboxes of Azure AD users:

- **AzureAdOAuth2TokenEndpoint (String)**
  
  The endpoint used to obtain an access token using OAuth 2.0 (see Authorizing the Coveo Connector to Access the Exchange Online Mailboxes of Your Azure AD Users).

- **AzureAdGraphApiEndpoint (String)**
  
  The endpoint used by the Azure AD Graph API to access directory data in the Windows Azure AD directory (see Authorizing the Coveo Connector to Access the Exchange Online Mailboxes of Your Azure AD Users).

- **AzureAdClientId (String)**
  
  The Azure AD client ID (see Authorizing the Coveo Connector to Access the Exchange Online Mailboxes of Your Azure AD Users).

- **AzureAdClientKey (String)**
  
  The Azure AD client key (see Authorizing the Coveo Connector to Access the Exchange Online Mailboxes of Your Azure AD Users).

- **OwnerOnlySecurity (Integer)**
  
  Whether to assign the mailboxes owner as the only allowed identity on document. The default value is `false`. Set it to `true` when you index the Exchange online mailbox of your Azure AD users.

- **AzureAdUseUpnAsMailboxOwner (Integer)**
  
  Whether to use the user principal name (UPN) as mailbox owner or the user primary email. The default value is `false`. Change the value to `true` when you want your Exchange users listed in Azure AD to be recognized as UPN identities.
LDAPSearchRoot (String)

Specifies to the connector where to start looking in Active Directory. When this parameter is not specified, the connector looks at the root of Active Directory, which can be extremely large. By specifying a value, you can refine the search (see "What Are LDAP Searches?" on page 1230).

**Example:** To search only within the organizational unit (OU) companynameOU within the domain corp.companyname.com, enter:

```
LDAP://OU=companynameOU, DC=corp, DC=companyname, DC=com
```

LDAPFilters (String)

Filter applied to the search of Active Directory in order to find mailboxes (see "What Are LDAP Searches?" on page 1230). Allows adding properties to the results the connector is looking for. The default filter is: `(mail=*)(objectclass=user)(objectclass=person)`.

This AND operation is performed on a few properties to find the maximum number of mailboxes without receiving any unwanted ones. If this filter is not specific enough, you can complete the filter by adding a value to the AND operation on the filter.

**Example:** When you enter the value `cn=JohnSmith` in the parameter, the resulting filter is: `(& (mail=*) (objectclass=user) (objectclass=person) (cn=JohnSmith))`

GroupLDAPFilters (String)

Parameter used to filter the AD group expansion when the `ExpandADGroups` is set to true. This parameter behaves like the `LDAPFilters` parameter.

TimeOut (Integer)

The number of seconds to wait for Microsoft Exchange to answer when the crawler performs a request. The default value is 30 seconds.

NbPrefabThread (Integer)

The number of threads that attempt to get changes ahead of time from the server. The default value is 2.

**Note:** Increasing this above the value of the `ConnectionLimit` parameter has no effect and may even reduce performance as more threads fight for the smaller amount of connections.

NbRefreshThreads (Integer)

The number of threads that consume the prefetched items. These will also need to connect to the Microsoft Exchange Server to download attachments. The default value is 2.

MaxNumberPrefabChanges (Integer)

Maximum number of items that can be stored in the prefetch cache. This cache is useful to reduce the delay between each query to Microsoft Exchange. The default value is 200.

Increasing this value increases performance, but also the amount of memory used by the connector. If the connector is running on a server with limited memory resources, lowering this number to 100 or 50 can prevent out of memory issues.
**BatchSize (Integer)**

Number of items to fetch per request made to the Microsoft Exchange Server. The default value is 50. The minimum value is 1 and the maximum 512. A small value forces the connector to make small but frequent queries to Microsoft Exchange. A larger value leads to larger and less frequent connections.

**IndexMailbox (Boolean)**

Determines if normal mailboxes should be indexed. This parameter only makes sense with Microsoft Exchange 2010 where archives also exist. The default value is true.

**IndexArchive (Boolean)**

Determines if Microsoft Exchange 2013 or 2010 archive mailboxes should be indexed. The default value is true.

**IndexOutbox (Boolean)**

Can be added to crawl the Outbox folder. This folder usually only temporarily contains emails before they are sent by the Exchange server. The default value is false.

**IndexJunkAttachments (Boolean)**

When set to true, the attachments of junk emails are indexed, otherwise they are ignored. The default value is false.

**SkipEmbeddedImageAttachment (Boolean)**

When set to true, the images embedded directly within the text of an email (like signature images) are skipped, otherwise they are indexed. The default value is true.

**UserDefinedFields (String)**

Can be added to retrieve user defined fields from Microsoft Exchange items. This string is in the following format Fieldtype:FieldName;FieldType:FieldName, etc. The FieldType value is taken directly from the Microsoft Exchange Form Designer. The FieldName value is the name of the field as entered in the Form Designer.

**ConnectionLimit (Integer)**

Can be added to increase performance. If you plan on increasing the number of threads in the connector, you will also need to increase this value. The suggested value is the sum of all the threads you want to be able to connect to Exchange, in all your sources. Increasing this value will increase the load on the Exchange Server. The default value is 2.

**OMCAdditionalIncludes (String)**

Parameter used to specify additional item classes to get. By default, the crawler gets the following types:

- IPM.Note
- IPM.Post
- IPM.Document
Additional fields must be separated by a semi-colon (;). These types are recursive.

**Example:** When the crawler gets IPM.Note, it also gets IPM.Note.Whatever.

**Note:** When you add a type and later remove it, the indexed items of that type will be deleted at the next rebuild.

**OMCExcludes (String)**

Parameter allowing to exclude particular item classes that are included by default or by the OMCAdditionalIncludes parameter. The exclusion is recursive.

**Example:** When you exclude IPM.Note, you also exclude IPM.Note.Whatever.

**Note:** When you exclude a type for which items are indexed, the indexed items of that type will be deleted at the next rebuild.

**IgnoreUnresolvedDeniedSecurities (Boolean)**

Can be added to allow the connector to keep crawling even after finding denied permissions that could not be resolved. This behavior could create a security hole, so this parameter should be used with caution. The default value is false.

**ResolveDisplayValuesWithContacts (Boolean)**

Can be added to allow the connector to perform a resolution of the email address values found on emails with the mailbox contacts. The default value is false.

**Example:** When the connector finds the To value jsmith <jsmith@companyname.com>, it looks into the contacts folder of this mailbox and tries to form a new value using the first and last name of the contact: John Smith <jsmith@companyname.com>.
ExpandADGroups (Boolean)

Can be added to allow the connector to perform an expansion of Active Directory groups it finds while looking for users (based on the LDAPSearchRoot and LDAPFilters parameters). The users found in these groups that have a mailbox are added to the list of mailboxes to crawl, even if they do not match the original LDAPSearchRoot or LDAPFilters. The default value is false.

MaxReceivedMessageSize (Integer)

The maximum size of messages (in bytes) received from the Exchange callback service that the Exchange crawler can accept. A message appears indicating when this parameter needs to be changed. The default value is 2048000. This parameter may need to be changed only for Exchange servers with very high email traffic.

CallbackServiceTimeout (Integer)

The number of seconds the Exchange crawler waits for the Exchange callback service to send a message or receive an answer. The default value is 60 seconds. You can increase this parameter if you receive timeout messages from the Exchange callback service. This parameter may need to be changed only for Exchange servers with very high email traffic.

Exchange2013ViewModelValue (String) CES 7.0.5989+ (October 2013)

For Exchange Server 2013 and Exchange Online, use this parameter to modify the default value of the ViewModel attribute in the OWA clickable URIs to ensure that the OWA URI is valid. When the OWA URI is invalid, end-users are not able to open Exchange search results in Outlook Web Access (OWA).

You can find the appropriate value to use for this parameter for your deployment as follows:

1. In Outlook Web Access, open an email message in a separate browser window or tab.
2. In the browser address bar, look for the ViewModel attribute value (example reported in the Microsoft documentation: _y$Ep).
3. When the ViewModel attribute value read from the URL is not the default (ReadMessageItem), enter it for the Exchange2013ViewModelValue parameter value.

Example: In the following clickable URI example, the ViewModel attribute uses the default value (ReadMessageItem):

https://exchange.server/owa/#viewmodel=ReadMessageItem&ItemID=12o378459749379375b yvyt7b3

IndexedContentScope (String) CES 7.0.6196+ (November 2013)

This parameter determines the type of content to index. The default is ServerOwnContent. The following table
lists available values.

<table>
<thead>
<tr>
<th>Values</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ServerOwnContent</td>
<td>Index all Exchange content except remote archives (Default).</td>
</tr>
<tr>
<td>Mailboxes</td>
<td>Index only mailboxes</td>
</tr>
<tr>
<td>LocalArchives</td>
<td>Index only local archives</td>
</tr>
<tr>
<td>RemoteArchives</td>
<td>Index only remote archives</td>
</tr>
</tbody>
</table>

### PowerShellEndpoint (String) CES 7.0.6684+ (May 2014)

Specifies the PowerShell endpoint of the Exchange server used by the connector to list all the mailboxes to crawl. The connector uses the LDAPSearchRoot parameter by default to expand starting addresses, but rather uses the `PowerShellEndpoint` parameter when it is defined.

For a Microsoft Exchange Online source like in the remote archive part of a hybrid deployment, you must specify the `PowerShellEndpoint` because in this case, Active Directory is not available, and consequently, LDAP searches cannot be used.

For the remote archive part in a hybrid deployment, although not obvious, you must connect PowerShell to the Exchange On-Premises Server to allow the connector to list the remote archives hosted in Exchange Online. This is because only the Exchange On-Premises Server can be queried to retrieve all mailboxes and to detect which of these mailboxes have its archive hosted on Exchange Online. The `PowerShellEndpoint` parameter value for an (local) Exchange On-Premises Server is typically in the following form:

https://exchange.mycompany.com/powershell

### Notes:

- The `PowerShellEndpoint` parameter is available starting with the CES 7.0.6684 May 2014 monthly release.
- On the Coveo Master server, the crawler is allowed to execute a PowerShell script when the PowerShell execution policy is set to `RemoteSigned` (see Using the `Set-ExecutionPolicy` Cmdlet).

### PowerShellUserName (String) CES 7.0.6684+ (May 2014)

### PowerShellUserPassword (String) CES 7.0.6684+ (May 2014)

When a CES user identity associated with a source for a remote part of an Exchange hybrid deployment cannot meet all the requirements to access all necessary services, you can use the `PowerShellUserName` and `PowerShellUserPassword` parameters to add a set of PowerShell credentials meeting the requirements (see Creating a Microsoft Exchange Crawling Account).

**Example:** You need to access Exchange Online EWS using an In Cloud user which is not synchronized with Active Directory (AD). Since this In Cloud user is not a valid AD user and cannot be a local Exchange On-Premises Server administrator, you must add the `PowerShellUserName` and `PowerShellUserPassword` parameters to the source to hold the PowerShell credentials meeting the requirements.
Note: Be aware that the PowerShellUserName and PowerShellUserPassword parameter strings are saved in clear text in the connector configuration file.

OnlyIndexActiveUserMailboxes (Boolean) CES 7.0.6830+ (July 2014)

When set to true, the default, the mailboxes of disabled users are not indexed. Set this parameter to false when you want to index disabled user mailboxes along with those of active users.

Note: The OnlyIndexActiveUserMailboxes parameter replaces the IndexMailboxUsersOnly obsolete parameter.

UseDefaultFiltersToFindMailboxes (Boolean) CES 7.0.6830+ (July 2014)

When set to true, the default, adds the default Coveo LDAP Filters to our LDAP Queries:

"(&(mail=*)(objectclass=user)(objectclass=person)"

Note: The UseDefaultFiltersToFindMailboxes parameter replaces the IndexMailboxUsersOnly obsolete parameter.

IgnoreRMSEmailBody (Boolean) CES 7.0.7433+ (February 2015)

Whether to ignore the body of emails protected by Microsoft rights Management Services (RMS) policies. The default value is true, meaning that RMS protected emails are not indexed.

RMSMessage (String) CES 7.0.7433+ (February 2015)

The message the crawler looks for to determine if emails are RMS protected or not. The default value is This message uses Microsoft Information Protection solutions. Open this item using an email application that supports protected messages. Only change this value when you modified the message replacing the body of RMS protected emails in Exchange.

IndexMailboxUsersOnly (Boolean) OBSOLETE CES 7.0.6767– (June 2014)

When set to false, the mailboxes of disabled users are indexed along with the mailboxes of active users. The default value is true, meaning that disabled users mailboxes are not indexed.

Note: The IndexMailboxUsersOnly parameter was available for CES 7.0.5556+ (June 2013) to CES 7.0.6767– (June 2014) inclusively, but its functionality is now replaced by two parameters: OnlyIndexActiveUserMailboxes and UseDefaultFiltersToFindMailboxes.

DateScopedCrawlingSinceXDays (Integer) CES 7.0.8225+ (March 2016)

Instructs to index only items with a modification date between now and the specified number of previous days. By default, there is no modification date filter. This parameter is useful to limit the size of a source when you do not need old items to be searchable.

Example: You want to index only items that have been modified over the last 2 years, so you set the DateScopedCrawlingSinceXDays parameter to 730 (days).
Note: You cannot set a value for the DateScopedCrawlingSinceXDays parameter when you use either of the DateScopedCrawlingRangeLowerLimit or DateScopedCrawlingRangeUpperLimit parameters.

**DateScopedCrawlingRangeLowerLimit** (String)

**DateScopedCrawlingRangeUpperLimit** (String) CES 7.0.8225+ (March 2016)

Indexes only items for which the modification date is equal or after (DateScopedCrawlingRangeLowerLimit parameter) or before (DateScopedCrawlingRangeUpperLimit parameter) the specified date entered in the MM/dd/yyyy format. These parameters, together or alone, are useful to limit the size of a source and allow you to split your Exchange content in 2 or more sources based on content modification dates.

**Example:** You use both the DateScopedCrawlingRangeLowerLimit or DateScopedCrawlingRangeUpperLimit parameters to create one Exchange source per previous year from 01/01/yyyy to 12/31/yyyy, and the DateScopedCrawlingRangeLowerLimit parameter to configure one source for the current year. Only the current year source needs to be regularly refreshed, reducing the load on your Exchange server.

*Note:* You cannot use either of the DateScopedCrawlingRangeLowerLimit or DateScopedCrawlingRangeUpperLimit parameters when you use the DateScopedCrawlingSinceXDays parameter.

Use the following procedure only when you want to modify one or more of the above hidden source parameters.

**To modify hidden Microsoft Exchange source parameters**

1. Refer to "Adding an Explicit Connector Parameter" on page 450 to add one or more Microsoft Exchange hidden source parameters.

2. For a new Microsoft Exchange source, access the Add Source page of the Administration Tool to modify the value of the newly added advanced parameter:
   a. Select Index > Sources and Collections.
   b. Under Collections, select the collection in which you want to add the source.
   c. Under Sources, click Add.
   d. In the Add Source page, edit the newly added advanced parameter value.

3. For an existing Microsoft Exchange source, access the Source: ... General page of the Administration Tool to modify the value of the newly added advanced parameter:
   a. Select Index > Sources and Collections.
   b. Under Collections, select the collection containing the source you want to modify.
   c. Under Sources, click the existing Microsoft Exchange source in which you want to modify the newly added advanced parameter.
   d. In the Source: ... General page, edit the newly added advanced parameter value.

**9.27.7.6 What Are LDAP Searches?**

Lightweight Directory Access Protocol (LDAP) searches are an important part of the Microsoft Exchange connector.
When the starting addresses https://servername or https://servername/exchange are used, a query is performed against Active Directory of the current domain to find the available mailboxes. The results should reflect all the users in the Active Directory who own a mailbox. Depending on the configuration of Active Directory, it is possible that the results do not match the anticipated results.

You can use the LDAPSearchRoot and LDAPFilters hidden advanced parameters of the Microsoft Exchange connector to fine tune the search (see "Modifying Hidden Microsoft Exchange Source Parameters" on page 1222).

Example: In the following LDAP search example that could be used for the LDAPSearchRoot parameter, the first part of the LDAP string is important, since it specifies the domain.

| LDAP://corp.mycompany.com/OU=MAIN,dc=corp,dc=mycompany,dc=com |

9.28 Microsoft Office 365 Support Information

The Coveo Enterprise Search (CES) connectors partially support products associated with Microsoft Office 365. The following list indicates the supported state of connectors for common Office 365 products.

- **SharePoint Online**
  
  You can index SharePoint Online content using the Microsoft SharePoint Connector (see "Microsoft SharePoint Connector" on page 1243).

  **Note:** Several quick setup topics are available for various SharePoint online environments (see "Microsoft SharePoint Source Quick Setups" on page 1247).

- **Exchange Online**
  
  You can index Exchange Online content using the Microsoft Exchange connector (see "Microsoft Exchange Connector" on page 1173).

- **OneDrive for Business**
  
  You can index OneDrive for Business content using the Microsoft OneDrive for Business Connector (see "Microsoft OneDrive for Business Connector" on page 1231).

Contact Coveo Support for more information.

9.29 Microsoft OneDrive for Business Connector

**CES 7.0.8047+ (December 2015)**

The Coveo connector for Microsoft OneDrive for Business (previously known as SkyDrive Pro) allows you to bring the information stored on OneDrives for Business contained in SharePoint personal sites (MySites) into the unified index so that end-users can easily access this content. The connector allows Coveo Enterprise Search (CES) to crawl and index OneDrives in SharePoint (2013 and Online) personal sites.
OneDrive for Business connector features

- Content indexing
  
The connector indexes all the OneDrive for Business content created or uploaded in OneDrive such as Word, Excel, PowerPoint, OneNote documents.

  **Note:** OneNote documents are not indexed by default. You need to install Microsoft Office 2010 Filter Pack (see Microsoft OneDrive for Business Connector Deployment Overview).

- Security
  
The OneDrive for Business connector supports security for SharePoint using Classic Mode or Claims Based authentication.
  
  - Classic Mode
    
The connector indexes permissions on OneDrive for Business items as SharePoint groups and Windows accounts.
    
    - When a user performs a query, returned results are only those to which his Windows account has access.
  
  - Claims Based (Windows [NTLM or Kerberos], ADFS)
    
The connector indexes permissions on OneDrive for Business items as SharePoint groups and Claims.
    
    - When a user performs a query, returned results are only those with permissions that match any of the Claims assigned to the user after he is successfully authenticated in SharePoint.

- Incremental refresh
  
  Once incremental refresh is enabled on a OneDrive for Business source, the OneDrive for Business connector automatically refreshes the content modified since the last incremental refresh run. This way, the index is always kept up to date.

9.29.1 Microsoft OneDrive for Business Connector Deployment Overview

The following procedure outlines the steps needed to deploy the Microsoft OneDrive for Business connector. The OneDrive for Business connector supports the two SharePoint versions containing OneDrive for Business (2013 and Online) as well as various authentication modes. The configuration steps depend on the configuration of your SharePoint environment.

**Note:** Since OneDrive for Business is part of SharePoint (2013 and Online), the OneDrive for Business connector deployment includes steps of the SharePoint connector deployment.

1. Validate that your environment meets the requirements:

   - Coveo license for the OneDrive for Business connector
     
     Your Coveo license must include support for the Microsoft OneDrive for Business connector to be able to use this connector.

   - (For SharePoint Online only) Configure DNS records for Office 365 at your DNS hosting provider.
a. Log in to Office 365 admin center with an administrator account.

b. In the navigation bar on the left, select Domains.

c. In the Manage domains page:
   i. Under Domain Name, select your corporate domain (not company.onmicrosoft.com) check box.
   ii. Next to the Action column, under the [domain name], click Domain settings.

d. In the [domain name] page, in the DNS records section, take note of the DNS records.

e. Configure these DNS records in your DNS host provider (see Create DNS records for Office 365 when you manage your DNS records).

f. In the [domain name] page, in the DNS records section, click the Troubleshoot domain link to ensure the DNS records were correctly configured.

- CES 7.0.8047+ (December 2015)

- ADFS requirements

When your SharePoint environment uses ADFS as a trusted identity provider, your ADFS setup must meet specific requirements (see “ADFS Server Requirements for a Claims Security Provider” on page 1330).

- Supported SharePoint version:
  - SharePoint Online
  - SharePoint 2013 (on-premises)

2. On your SharePoint farm:

   a. Select or create a user that the connector will use to crawl your OneDrive for Business content. Refer to the following table to identify the required type of user for your type of SharePoint environment.

<table>
<thead>
<tr>
<th>SharePoint environment</th>
<th>SharePoint Web Application Enabled authentication</th>
<th>Type of user</th>
<th>User format</th>
</tr>
</thead>
<tbody>
<tr>
<td>Classic (2013)</td>
<td>Windows</td>
<td>Windows account</td>
<td>domain\username or <a href="mailto:username@domain.com">username@domain.com</a></td>
</tr>
<tr>
<td>Claims (2013)</td>
<td>Windows</td>
<td>Windows account</td>
<td></td>
</tr>
<tr>
<td></td>
<td>ADFS</td>
<td>ADFS SSO</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Okta</td>
<td>Okta SSO</td>
<td><a href="mailto:username@domain.com">username@domain.com</a></td>
</tr>
</tbody>
</table>
**b.** Grant appropriate SharePoint permissions to the crawling account you selected to ensure access to all the content that you want to index (see Granting SharePoint Permissions to the Crawling Account).

3. **On the Coveo Master server, in the Administration Tool:**
   a. *(When you want to index OneNote files)* Setup IFilters:
      i. Download and install the Microsoft Office 2010 Filter pack (see Microsoft Office 2010 Filter Packs).
      
      **Note:** Ensure your CES server meets the system requirements.
      
      ii. Load IFilter mapping (see "Applying IFilters to Document Types" on page 482).
      
      **Notes:**
      - OneNote pages are inside OneNote sections when the sections are separate documents.
      - Ignore the .onetoc2 document type as these files do not contain any data by filtering them out. OneNote files are shortcuts created by OneNote that are not relevant.

   b. **Configure the user identity**
   
   Once the crawling account has been set up, you must create a CES user identity for this account.

   c. **When indexing OneDrive for Business content inside SharePoint Online,** you must install the Windows Azure AD module on the Coveo Master server because it is needed by the Office 365 security provider (see "Installing the Windows Azure AD Module for Windows PowerShell" on page 1331).

   d. **Referring to the following table,** create the security providers required for your SharePoint environment following the order in the numerical icons.

<table>
<thead>
<tr>
<th>Required security provider type</th>
<th>Online</th>
<th>2013 on-premises</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>Office 365 Native</td>
</tr>
<tr>
<td>Active Directory</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Required security provider type</td>
<td>Online</td>
<td>2013 on-premises</td>
</tr>
<tr>
<td>---------------------------------</td>
<td>--------</td>
<td>-----------------</td>
</tr>
<tr>
<td></td>
<td>Office 365 Native</td>
<td>SSO ADFS</td>
</tr>
<tr>
<td>Claims for SharePoint on-premises</td>
<td>2</td>
<td></td>
</tr>
<tr>
<td>Claims for SharePoint Online</td>
<td>1 OR</td>
<td>1 OR</td>
</tr>
<tr>
<td>Claim to Email for SharePoint Online</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>Office 365</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>SharePoint</td>
<td>3</td>
<td>3</td>
</tr>
</tbody>
</table>

**Note:** When an Active Directory security provider is required, use the out-of-the-box Active Directory security provider.

e. Configure and index the Microsoft OneDrive for Business source

The Coveo connector needs to know details about your Microsoft SharePoint server or farm to be able to index its content (see "Configuring and Indexing a Microsoft OneDrive for Business Source" on page 1235).

### 9.29.2 Configuring and Indexing a Microsoft OneDrive for Business Source

A source defines a set of configuration parameters to extract and index Microsoft OneDrive for Business content. This topic describes how to create a source using the OneDrive for Business connector.

**To configure and index a Microsoft OneDrive for Business Source**

1. On the Coveo server, access the Administration Tool.
2. Select **Index > Sources and Collections**.
3. In the **Collections** section:
   a. Select an existing collection in which you want to add the new source.
      OR
   b. Click **Add** to create a new collection.
4. In the **Sources** section, click **Add**.
   The **Add Source** page that appears is organized in three sections.
5. In the **General Settings** section of the **Add Source** page:
a. Enter the appropriate value for the following required parameters:

**Name**

Enter a descriptive name of your choice for this source.

**Example:** OneDrive for Business

**Source Type**

The connector used by this source. In this case, select OneDrive for Business.

**Addresses**

Depending on your SharePoint environment:

- For SharePoint Online: The URL of the SharePoint site collection regrouping all the personal sites (in which are located the OneDrives for Business) that you want to index.

  **Example:** https://domain-my.sharepoint.com

- For SharePoint 2013: The URL of the Web Application you want to index personal sites from.

  **Example:** https://farm:8080/

**Refresh Schedule**

Time interval at which the source is automatically refreshed to keep the index content up-to-date.
Note: The default Every Day option is typically good, but when your OneDrive for Business content changes frequently within a day, after creating your source, you should schedule incremental refresh at significantly shorter time interval to continuously index ongoing OneDrive for Business content changes. You can then consider to refresh the source weekly by selecting the Every Sunday option.

b. Review the value for the following parameters that often do not need to be modified:

Rating

Change this value only when you want to globally change the rating associated with all items in this source relative to the rating to other sources.

Example: If this source was for a legacy Intranet, you may want to set this parameter to Low, so that in the search interface, results from this source appear later in the list compared to those from other sources.

Document Types

If you defined custom document type sets, ensure to select the most appropriate for this source.

Active Languages

If you defined custom active language sets, ensure to select the most appropriate for this source.

Fields

If you defined custom field sets, ensure to select the most appropriate for this source.

6. In the Specific Connector Parameters & Options section of the Add Source page, review if you need to change the parameter default values:

<table>
<thead>
<tr>
<th>Authentication Type</th>
<th>WindowsClassic</th>
<th>Options</th>
</tr>
</thead>
<tbody>
<tr>
<td>Parameters</td>
<td>Add Parameter</td>
<td>Index subfolders</td>
</tr>
</tbody>
</table>

a. In the Authentication Type drop-down list, refer to the following table to select the authentication type value corresponding to your SharePoint environment and the type of User Identity that you assigned to this source (see Microsoft OneDrive for Business Connector Deployment Overview).

<table>
<thead>
<tr>
<th>SharePoint environment</th>
<th>User identity type</th>
<th>Option to select</th>
</tr>
</thead>
<tbody>
<tr>
<td>Classic</td>
<td>Windows account (SharePoint 2010 default)</td>
<td>WindowsClassic</td>
</tr>
</tbody>
</table>
b. In the **Parameters** section, click **Add Parameter** when you want to show and configure advanced hidden source parameters (see "Modifying Hidden Microsoft OneDrive for Business Source Parameters" on page 1240).

**Example:** In the case of an ADFS environment, when the **Authentication Type** parameter value is either **AdfsUnderClaims** or **SpOnlineFederated**, you must add ADFS related hidden parameters (see "ADFS Related Parameters" on page 1240).

<table>
<thead>
<tr>
<th>SharePoint environment</th>
<th>User identity type</th>
<th>Option to select</th>
</tr>
</thead>
<tbody>
<tr>
<td>Claims</td>
<td>Windows account (SharePoint 2013 default)</td>
<td>WindowsUnderClaims</td>
</tr>
<tr>
<td>ADFS federated account</td>
<td>AdfsUnderClaims</td>
<td></td>
</tr>
<tr>
<td>Online</td>
<td>Native Office 365 account</td>
<td>SpOnlineNative</td>
</tr>
<tr>
<td></td>
<td>Single Sign-On Office 365 account</td>
<td>SpOnlineFederated</td>
</tr>
</tbody>
</table>

Notes: You can configure the security provider to operate when multiple ADFS servers are used to authenticate users in SharePoint. [more]

c. In the **Option** section:

**Index Subfolders**

Keep this check box selected (recommended). By doing so, all subfolders from the specified server address are indexed.

**Index the document's metadata**

When selected, CES indexes all the document metadata, even metadata that are not associated with a field. The orphan metadata are added to the body of the document so that they can be searched using free text queries.

When cleared (default), only the values of system and custom fields that have the **Free Text Queries** attribute selected will be searchable without using a field query.
Example: A document has two metadata:

- LastEditedBy containing the value Hector Smith
- Department containing the value RH

In CES, the custom field CorpDepartment is bound to the metadata Department and its Free Text Queries attribute is selected.

When the Index the document's metadata option is cleared, searching for RH returns the document because a field is indexing this value. Searching for hector does not return the document because no field is indexing this value.

When the Index the document's metadata option is selected, searching for hector also returns the document because CES indexed orphan metadata.

Document's addresses are case-sensitive

Leave the check box cleared. This parameter needs to be checked only in rare cases for case sensitive systems in which distinct documents may have the same file name but with different casing.

Generate a cached HTML version of indexed documents

When you select this check box (recommended), at indexing time, CES creates HTML versions of indexed documents. In the search interfaces, users can then more rapidly review the content by clicking the Quick View link rather than opening the original document with the original application. Consider clearing this check box only if you do not want to use Quick View links.

Open results with cached version

Leave this check box cleared (recommended) so that in the search interfaces, the main search result link opens the original document with the original application. Consider selecting this check box only when you do not want users to be able to open the original document but only see the HTML version of the document as a Quick View. In this case, you must also select Generate a cached HTML version of indexed documents.

7. In the Security section of the Add Source page:

   a. In the Authentication drop-down list, select the user identity that you created for the Microsoft SharePoint farm (see Microsoft OneDrive for Business Connector Deployment Overview).
b. In the **Security Provider** drop-down list, select the SharePoint security provider that you created for this OneDrive for Business source.

c. Click **Save** to save the source configuration and consider revising advanced source parameters before starting indexing the new source (see "Modifying Hidden Microsoft OneDrive for Business Source Parameters" on page 1240).

OR

d. Click **Save and Start** to save and start indexing immediately.

**Note:** When your SharePoint Web Application uses Claims, the first time the SharePoint .NET search interface is accessed, the first time setup page appears to let you enter your Claims information and allow access to the search interface (see Coveo .NET Front-End First Time Setup).

What's Next?

Set an incremental refresh schedule for your source.

9.29.2.1 Modifying Hidden Microsoft OneDrive for Business Source Parameters

The **Add Source** and **Source: ... General** pages of the Administration Tool present the parameters with which you can configure the connector for most Microsoft OneDrive for Business setups. More advanced and more rarely used parameters are hidden. You can choose to make one or more of these parameters appear in the **Add Source** and **Source: ... General** pages of the Administration Tool so that you can change their default value.

The following list describes the available advanced hidden parameters for Microsoft OneDrive for Business sources. The parameter type (integer, string…) appears between parentheses following the parameter name.

9.29.2.1.1 ADFS Related Parameters

The following ADFS related parameters are only required when the source **Authentication Type** parameter is either **AdfsUnderClaims** or **SpOnlineFederated**:

**AdfsServerUrl (String)**

URL of the AD FS server for which a trust is established with SharePoint.
Note: The Microsoft OneDrive for Business connector supports indexing SharePoint online configured with Okta (see "SharePoint Online (Okta SSO) [Claims] Source Quick Setup" on page 1265).

In this case, you must add the AdfsServerUrl hidden parameter to the source and set the value to the full path to your SharePoint Online ActiveClientSignInUrl that should be in the form:

https://acme.okta.com/app/office365/abcdefgGWUMNWLWYGXF/sso/wsfed/active

You can find your SharePoint Online ActiveClientSignInUrl in Okta, in the sign on instructions of the Microsoft Office 365 application:

1. With an administrator account, log in into Okta.
2. In the top menu, click Admin.
3. In the administration panel, select Applications > Applications.
4. In the Applications page, click Microsoft Office 365.
5. In the Microsoft Office 365 page, select the Sign On tab.
6. In the Sign On tab, under Sign On Methods section, click View Setup Instructions.
7. The ActiveClientSignInUrl is the value next to ActiveLogOnUrl.

Ensure that you also set this ActiveClientSignInUrl for the Claims Security provider and the SharePoint source (see Creating a Claims Security Provider for SharePoint Online and Creating a SharePoint Security Provider).

SharePointTrustIdentifier (String)

The Relying Party Trust identifier for the SharePoint ADFS server (see "Finding the Relying Party Trust Identifier for a SharePoint ADFS server" on page 112).

The following parameters are required only when multiple ADFS servers are used to authenticate users in SharePoint:

IdentityProviderServerUrl (String)

The URL of the ADFS server which is used as an Identity Provider for the ADFS server trusted by SharePoint.

AdfsServerTrustIdentifier (String)

Trust Identifier for the SharePoint AD FS Server. Enter the Relying Party Trust identifier for the SharePoint web application (see "Finding the Relying Party Trust Identifier for a SharePoint Web Application" on page 111).

9.29.2.1.2 Other Parameters

AllowBasicAuthentication (Boolean)

Select the AllowBasicAuthentication option only when basic authentication is enabled on the web application to index and specifically want to use this authentication mode. The default value is false.

It is recommended to use this authentication method only with a secured connection (HTTPS) because the user name and password are passed in clear text in the URL.
AuthenticationRealmUrl (String)

(For SharePoint Online only) Add this hidden parameter only when your SharePoint environment includes an online authentication service on a separate server, in which case you enter the authentication server URL in the form https://domain.sharepoint.com.

EnableOfficeIntegration (Boolean)

Whether to enable the office integration in the .NET UI or not. This will change the clickable URI to open documents directly in Office. The default value is true.

IndexListFolders (Boolean)

Whether to index List Folders or not. The default value is false, because Web folders are not accessible via the browser, only from Windows Explorer. Set to true when you want to see the List Folders in search results.

ServerNameAlias (String)

Specifies a server name that overrides the one from which documents are downloaded in the index. This parameter is useful to have query results point to a server other than the one used for indexing.

Example: Three network load balanced (NLB) SharePoint front-end servers handle the end-users requests and your source crawls a fourth mirror server to not impact performance for users. In this case, you add the ServerNameAlias parameter and set the value to the NLB URL to replace the IP address in the index.

To modify hidden Microsoft OneDrive for Business source parameters

1. Refer to "Adding an Explicit Connector Parameter" on page 450 to add one or more Microsoft OneDrive for Business hidden source parameters.

2. For a new Microsoft OneDrive for Business source, access the Add Source page of the Administration Tool to modify the value of the newly added advanced parameter:
   a. Select Index > Sources and Collections.
   b. Under Collections, select the collection in which you want to add the source.
   c. Under Sources, click Add.
   d. In the Add Source page, edit the newly added advanced parameter value.

3. For an existing Microsoft OneDrive for Business source, access the Source: ... General page of the Administration Tool to modify the value of the newly added advanced parameter:
   a. Select Index > Sources and Collections.
   b. Under Collections, select the collection containing the source you want to modify.
   c. Under Sources, click the existing Microsoft OneDrive for Business source in which you want to modify the newly added advanced parameter.
   d. In the Source: ... General page, edit the newly added advanced parameter value.
9.30 Microsoft SharePoint Connector

**CES 7.0.6767+ (June 2014)**

The second generation Coveo connector for Microsoft SharePoint allows you to bring the information stored on one or multiple SharePoint farms (tenants in SharePoint Online) into the unified index so that end-users can easily access this content. The connector allows Coveo Enterprise Search (CES) to crawl and index a complete SharePoint farm or specific farm sections, such as Web Applications, site collections, websites, lists, and document libraries.

**Note:** The document in this section describes the second generation SharePoint connector.

**CES 7.0.6830+ (July 2014)** The original SharePoint connector is still available and was renamed SharePoint Legacy connector.

**CES 7.0.7433+ (February 2015)** A tool to convert your SharePoint Legacy sources to SharePoint sources is available. The SharePoint Converter Tool is pretty useful when you want to take full advantage of the improved SharePoint connector without having to recreate all your SharePoint Legacy sources. Contact Coveo Support to get the SharePoint Converter Tool.

9.30.1 Comparison With the Legacy Connector

The second generation SharePoint connector has been completely rewritten to provide similar features as the SharePoint Legacy connector with the bonus of a significantly improved crawling performance thanks to multi-threading and optimized API communications. For supported SharePoint versions, Coveo recommends to use the new SharePoint connector to create or migrate SharePoint sources.

The following table highlights the differences between the two connectors.

<table>
<thead>
<tr>
<th>Comparison aspect</th>
<th>New SharePoint connector</th>
<th>SharePoint Legacy connector</th>
</tr>
</thead>
<tbody>
<tr>
<td>Crawling performance</td>
<td>Significantly improved</td>
<td>Good</td>
</tr>
<tr>
<td>Multi-threading</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Refresh subtree</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Claims form authentication</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Unpublished items</td>
<td>Not indexed</td>
<td>Indexed</td>
</tr>
</tbody>
</table>
9.30.2 Connector Features Summary

<table>
<thead>
<tr>
<th>Features</th>
<th>Supported</th>
<th>Additional information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Searchable content types</td>
<td>✅</td>
<td>Farms (tenants in SharePoint Online), Web applications, site collections, sites, user profiles*, personal websites*, lists, list items, list item attachments, document libraries, document sets, documents, Web parts¹, and microblog posts and replies.</td>
</tr>
<tr>
<td>Content update</td>
<td>Incremental refresh ✅</td>
<td>Full refresh or rebuild is needed to retrieve deleted user profiles¹.</td>
</tr>
<tr>
<td></td>
<td>Full refresh ✅</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Rebuild ✅</td>
<td></td>
</tr>
<tr>
<td>Document-level security</td>
<td>✅</td>
<td></td>
</tr>
</tbody>
</table>

* - Not available in Microsoft SharePoint Foundation.

¹ - Not all Web parts are available in Microsoft SharePoint Foundation 2010 (see Overview of Web Parts available in SharePoint Foundation 2010).

9.30.3 Features

- Content indexing
  - Indexing all SharePoint content
    - Farms (tenants in SharePoint Online) and Web Applications
    - Site collections, websites, and subsites
    - Lists, list items, and list item attachments

  **Note:** CES 7.0.8225+ (March 2016) SharePoint Online lists, list items, and list item attachments are indexed.

    - Document libraries, documents, and document sets
    - User profiles and personal websites
Note: User profiles and personal websites are not available in Microsoft SharePoint Foundation.

- Microblog posts and replies
- CES 7.0.7022+ (September 2014) Web Parts Pages
  
  Note: Not all Web parts are available in Microsoft SharePoint Foundation 2010 (see Overview of Web Parts available in SharePoint Foundation 2010).

- CES 7.0.7022+ (September 2014) Social tags

  ○ HTTP over SSL (HTTPS) support

  You can use the SharePoint connector to index a SharePoint site that uses HTTPS.

- Security

  The SharePoint connector supports security for SharePoint Web Applications using Classic Mode or Claims Based authentication.

  ○ Classic Mode

    The connector indexes permissions on SharePoint items as SharePoint groups and Windows accounts.

    - When a user performs a query, returned results are only those to which his Windows account has access.

    - Users can perform queries from any Coveo search interface.

  ○ Claims Based (Windows [NTLM or Kerberos], ADFS)

    The connector indexes permissions on SharePoint items as SharePoint groups and Claims.

    - When a user performs a query, returned results are only those with permissions that match any of the Claims assigned to the user after he is successfully authenticated in SharePoint.

    - Users can perform queries from any Coveo .NET Front-End search interface:

      ○ When searching from within SharePoint using the Coveo search box, the user is already authenticated in SharePoint and his Claims are available to the Coveo search interface. This means that search queries can be performed using the Claims assigned to the user.

      ○ Claims users can also perform searches for secured SharePoint content from Coveo search interfaces outside SharePoint without having to log in to the search interface when the search interface is configured for SSO (see "Manually Configuring a .NET Search Interface Claims SSO for an On-Premises SharePoint" on page 178).

- CES 7.0.9093+ (September 2017) Users can perform queries from any Coveo JavaScript search interface (see "Coveo JavaScript Search Framework" on page 144 and "Allowing a JavaScript Search Page to Retrieve SharePoint Claims" on page 1316).

- Incremental refresh
Once incremental refresh is enabled on a SharePoint source, the SharePoint connector automatically refreshes the content modified since the last incremental refresh run. This way, the index is always kept up to date.

**Notes:**

- **CES 7.0.9434+ (September 2018)** A change in the URI of SharePoint documents will cause an incremental refresh to add duplicate documents to your index. A full refresh (recommended) or rebuild is required to remove those duplicates and prevent the issue from happening again.

- **CES 7.0.8541+ (September 2016)** The incremental refresh takes account of added and modified user profiles. A source full refresh or rebuild is required to update deleted user profiles.

- **CES 7.0.8388– (June 2016)** The incremental refresh does not take account of user profile changes.

- **SharePoint Integration:**
  - Installation of Coveo Web Service on the SharePoint server to provide more crawling functions
  - Installation of the Coveo search box to replace the SharePoint search box
  - Installation of Coveo search interfaces on the SharePoint server

- **Intranet and SharePoint** search interface features related to the SharePoint connector:
  - Search results folding for the following SharePoint items:
    - Blog posts and their comments
    - Discussion board threads
    - Document sets and their items
  - The **Document Sets** facet appears, listing all document sets included in the results when one or more document set items match the query.
  - Search results referring to a document link in SharePoint are now identified with a special icon.

- **CES 7.0.9272+ (March 2018)** Okta single sign-on authentication is supported (see Okta Single Sign-On Provider for SharePoint On-Premises).

**Note on exclusion filters**

The SharePoint connector does not expand filtered items, meaning that the connector only expands and indexes items that were not precedentely excluded by a filter.

When you want to exclude a specific container but include its sub-items, you must use a script. Contact Coveo Support for assistance.
Feature History

<table>
<thead>
<tr>
<th>CES version</th>
<th>Monthly release</th>
<th>Features</th>
</tr>
</thead>
<tbody>
<tr>
<td>7.0.9272</td>
<td>March 2018</td>
<td>Support for SharePoint on-premises SSO authentication with Okta [more]</td>
</tr>
<tr>
<td>7.0.8541</td>
<td>September 2016</td>
<td>Support for SharePoint 2016</td>
</tr>
<tr>
<td>7.0.7433</td>
<td>February 2015</td>
<td>Introduction of the SharePoint Converter Tool</td>
</tr>
<tr>
<td>7.0.7022</td>
<td>September 2014</td>
<td>Support for social tags and Web Parts Pages</td>
</tr>
</tbody>
</table>
| 7.0.6942    | August 2014     | - Indexing and folding for document sets
              - Incremental refresh for web files and document sets
              - Refresh/delete a specific SharePoint section |
| 7.0.6830    | July 2014       | - Support for incremental refresh
              - Selectable crawling scope [more] |
| 7.0.6767    | June 2014       | Introduction of this second generation SharePoint connector. |

9.30.4 Microsoft SharePoint Source Quick Setups

The second generation of Coveo connector for SharePoint and the OneDrive for Business connector [CES 7.0.8047+ (December 2015)] support several SharePoint versions and features as well as various authentication modes. The Coveo components and parameter values required to create SharePoint and OneDrive for Business sources vary depending on the SharePoint environment. The SharePoint and OneDrive for Business connectors documentation may consequently appear somewhat complex because it addresses all aspects of numerous SharePoint environment combinations.

The configuration of the components required to create a source for a given common SharePoint environment is however often simple for an administrator that is familiar with the Coveo Enterprise Search (CES) source creation process.

The topics in this section outline the required components and parameters to create a source for a few common SharePoint environments. Parameters not mentioned should be left to their default values.

In the table of contents, each quick setup title gives information on the SharePoint environment and the CES security configuration, helping you choosing the quick setup that best suits your needs.

Example: **Online** (Federated - ADFS) [Claims]

- The first part (in red) is the SharePoint deployment type/installation (either online or on-premises).
- The second part in parentheses (in blue) is the user authentication in SharePoint.
- The last part in square brackets (in green) is the user authentication in the Coveo search interface.

9.30.4.1 SharePoint 2016/2013/2010 On-Premises (Windows Classic) [AD] Source Quick Setup

[www.coveo.com](http://www.coveo.com)
1. Validate that your environment meets the requirements:
   - (For SharePoint 2010 and 2013) CES 7.0.6767+ (June 2014)
   OR
   - (For SharePoint 2016) CES 7.0.8541+ (September 2016)
   OR
   - (For Microsoft OneDrive for Business) CES 7.0.8047+ (December 2015)

   **Note:** You can check your CES version from the Administration Tool.

   - Your Coveo license includes the Microsoft SharePoint or Microsoft OneDrive for Business connector.

2. Create a user identity with a dedicated Windows account that has access to all the SharePoint content that you want to index.

<table>
<thead>
<tr>
<th>Key parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>You must name your user identity.</td>
</tr>
<tr>
<td>User</td>
<td>In the domain\username or <a href="mailto:username@domain.com">username@domain.com</a> form.</td>
</tr>
<tr>
<td>Password</td>
<td>The corresponding password.</td>
</tr>
</tbody>
</table>

3. (Not for OneDrive for Business sources) On your SharePoint farm, install the Coveo web service and optionally the search box, and search interface (see "Installing the Coveo Web Service, Search Box, and Search Interface into SharePoint" on page 1309).

4. Ensure that the crawling account of your user identity has appropriate permissions, the crawling account must:
- Be a member of the SharePoint farm administrators group (see "Adding the Crawling Account to the SharePoint Farm Administrators Group" on page 105)
- Have the Read permission for the site collection(s) that you want to index (see "Adding the SharePoint Website Read Permission" on page 101).

5. Create a SharePoint security provider. [more]

<table>
<thead>
<tr>
<th>Key parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>You must name your security provider.</td>
</tr>
<tr>
<td>Security Provider Type</td>
<td>SharePoint</td>
</tr>
<tr>
<td>User Identity</td>
<td>The user identity you just created.</td>
</tr>
<tr>
<td>Active Directory Security Provider</td>
<td>The default Active Directory security provider.</td>
</tr>
<tr>
<td>Security Provider for SharePoint Users</td>
<td>None</td>
</tr>
<tr>
<td>SharePoint Server Url</td>
<td>The URL of the SharePoint web application where the Coveo SharePoint Web Service is installed in the form http://SharePoint_server:[WebApp_port]</td>
</tr>
<tr>
<td>Authentication Type</td>
<td>WindowsClassic</td>
</tr>
</tbody>
</table>

6. Create a SharePoint or OneDrive for Business source.

<table>
<thead>
<tr>
<th>Key parameter</th>
<th>SharePoint</th>
<th>OneDrive for Business</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>You must name your source.</td>
<td></td>
</tr>
<tr>
<td>Source Type</td>
<td>SharePoint (x64)</td>
<td></td>
</tr>
<tr>
<td>Addresses</td>
<td>The URL for the SharePoint farm sections that you want to index in the form https://SharePoint_server[:port]/path, where [path] is needed only when you want index a specific site collection, list, etc.</td>
<td>The URL for the SharePoint web application that you want to index in the form https://SharePoint_server:[WebApp_port].</td>
</tr>
<tr>
<td>Authentication Type</td>
<td>WindowsClassic</td>
<td></td>
</tr>
<tr>
<td>Authentication</td>
<td>The user identity you just created.</td>
<td></td>
</tr>
<tr>
<td>Security Provider</td>
<td>The SharePoint security provider you just created.</td>
<td></td>
</tr>
</tbody>
</table>
7. Rebuild the source and validate that documents are indexed.

9.30.4.2 SharePoint 2016/2013/2010 On-Premises (Windows Under Claims) [Claims] Source Quick Setup

1. Validate that your environment meets the requirements:
   
   - (For SharePoint 2010 and 2013) **CES 7.0.6767+ (June 2014)**
     
   OR
   
   - (For SharePoint 2016) **CES 7.0.8541+ (September 2016)**
     
   OR
   
   - (For Microsoft OneDrive for Business) **CES 7.0.8047+ (December 2015)**
     
   **Note:** You can check your CES version from the Administration Tool.

   - Your Coveo license includes the Microsoft SharePoint or Microsoft OneDrive for Business connector.

2. Create a user identity with a dedicated Windows account that has access to all the SharePoint content that you want to index.

<table>
<thead>
<tr>
<th>Key parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>You must name your user identity.</td>
</tr>
<tr>
<td>User</td>
<td>In the <code>domain\username</code> or <code>username@domain.com</code> form.</td>
</tr>
<tr>
<td>Password</td>
<td>The corresponding password.</td>
</tr>
</tbody>
</table>

3. (Not for OneDrive for Business sources) On your SharePoint farm, install the Coveo web service and optionally the search box, and search interface (see "Installing the Coveo Web Service, Search Box, and Search Interface into SharePoint" on page 1309).

4. Ensure that the crawling account of your user identity has appropriate permissions, the crawling account must:
- Be a member of the SharePoint farm administrators group (see "Adding the Crawling Account to the SharePoint Farm Administrators Group" on page 105)

- Have the Read permission for the site collection(s) that you want to index (see "Adding the SharePoint Website Read Permission" on page 101).

5. Create a Claims for SharePoint on-premises security provider. [more]

<table>
<thead>
<tr>
<th>Key parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>You must name your security provider.</td>
</tr>
<tr>
<td>Security Provider Type</td>
<td>Claims for SharePoint On-premises</td>
</tr>
<tr>
<td>User Identity</td>
<td>The user identity you just created.</td>
</tr>
<tr>
<td>SharePoint Web Application Url</td>
<td>The URL of the SharePoint web application using Claims-based</td>
</tr>
<tr>
<td></td>
<td>authentication in the <a href="http://SharePointServer%5B:port%5D/form">http://SharePointServer[:port]/form</a>.</td>
</tr>
<tr>
<td>Web Application supports NTLM Claims Authentication</td>
<td>Selected</td>
</tr>
<tr>
<td>Allow Complex Identities</td>
<td>Selected</td>
</tr>
</tbody>
</table>

6. Create a SharePoint security provider. [more]

<table>
<thead>
<tr>
<th>Key parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>You must name your security provider.</td>
</tr>
<tr>
<td>Security Provider Type</td>
<td>SharePoint</td>
</tr>
<tr>
<td>User Identity</td>
<td>The user identity you just created.</td>
</tr>
<tr>
<td>Active Directory Security Provider</td>
<td>The default Active Directory security provider.</td>
</tr>
<tr>
<td>Security Provider for SharePoint Users</td>
<td>The Claims for SharePoint on-premises security provider you just created.</td>
</tr>
<tr>
<td>SharePoint Server Url</td>
<td>The URL of the SharePoint web application where the Coveo SharePoint Web Service is installed in the form http://SharePoint_server:[WebApp_port]</td>
</tr>
<tr>
<td>Authentication Type</td>
<td>WindowsUnderClaims</td>
</tr>
</tbody>
</table>

7. Create a SharePoint or OneDrive for Business source.
### Key Parameter

<table>
<thead>
<tr>
<th>Key parameter</th>
<th>SharePoint</th>
<th>OneDrive for Business</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>You must name your source.</td>
<td></td>
</tr>
<tr>
<td>Source Type</td>
<td>SharePoint (x64)</td>
<td>OneDrive for Business</td>
</tr>
<tr>
<td>Addresses</td>
<td>The URL for the SharePoint farm sections that you want to index in the form <code>https://SharePoint_server[:port]/path</code>, where <code>[path]</code> is needed only when you want to index a specific site collection, list, etc.</td>
<td>The URL for the SharePoint web application that you want to index in the form <code>https://SharePoint_server:[WebApp_port]</code>.</td>
</tr>
<tr>
<td>Authentication Type</td>
<td>WindowsUnderClaims</td>
<td></td>
</tr>
<tr>
<td>Authentication</td>
<td>The user identity you just created.</td>
<td></td>
</tr>
<tr>
<td>Security Provider</td>
<td>The SharePoint security provider you just created.</td>
<td></td>
</tr>
</tbody>
</table>

8. Rebuild the source and validate that documents are indexed.

What's Next?

- *(For SharePoint sources only)* When you provide a Coveo .NET Front-End search interface residing outside SharePoint and want users to be able to find Claims-secured SharePoint content without having to log in again to SharePoint, configure the search interface to manage single sign-on.

- **CES 7.0.9093+ (September 2017)** *(For SharePoint on-premises sources only)* When you provide a Coveo JavaScript search interface and want to leverage SharePoint claims for content security, install the Coveo Claims Security Module, among other things (see "Allowing a JavaScript Search Page to Retrieve SharePoint Claims" on page 1316).

9.30.4.3 SharePoint 2016/2013/2010 On-Premises (ADFS Under Claims) [Claims] Source Quick Setup
1. Validate that your environment meets the requirements:
   - (For SharePoint 2010 and 2013) CES 7.0.6767+ (June 2014)
   - (For SharePoint 2016) CES 7.0.8541+ (September 2016)
   - (For Microsoft OneDrive for Business) CES 7.0.8047+ (December 2015)
   
   **Note:** You can check your CES version from the Administration Tool.

   - Your Coveo license includes the Microsoft SharePoint or Microsoft OneDrive for Business connector.
   - Your ADFS setup meets Coveo requirements. [more]

2. Create a user identity with a dedicated Windows account that has access to all the SharePoint content that you want to index.

<table>
<thead>
<tr>
<th>Key parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>You must name your user identity.</td>
</tr>
<tr>
<td>User</td>
<td>In the domain\username or <a href="mailto:username@domain.com">username@domain.com</a> form.</td>
</tr>
<tr>
<td>Password</td>
<td>The corresponding password.</td>
</tr>
</tbody>
</table>
a. (Not for OneDrive for Business sources) On your SharePoint farm, install the Coveo web service and optionally the search box, and search interface (see "Installing the Coveo Web Service, Search Box, and Search Interface into SharePoint" on page 1309).

3. Ensure that the crawling account of your user identity has appropriate permissions, the crawling account must:
   - Be a member of the SharePoint farm administrators group (see "Adding the Crawling Account to the SharePoint Farm Administrators Group" on page 105)
   - Have the Read permission for the site collection(s) that you want to index (see "Adding the SharePoint Website Read Permission" on page 101).

4. Create a Claims for an on-premises SharePoint security provider. [more]

<table>
<thead>
<tr>
<th>Key parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>You must name your security provider.</td>
</tr>
<tr>
<td>Security Provider Type</td>
<td>Claims for SharePoint On-premises</td>
</tr>
<tr>
<td>User Identity</td>
<td>When you want to use a Claims-aware Coveo Search, select a user identity of any Windows account that can be used to authenticate to ADFS (see &quot;Configuring the Claims-Aware Coveo Search Application&quot; on page 183). Otherwise, select the user identity you just created.</td>
</tr>
<tr>
<td>SharePoint Web Application Url</td>
<td>The URL of the SharePoint web application using Claims-based authentication in the <a href="http://SharePointServer%5B:port%5D/">http://SharePointServer[:port]/</a> form.</td>
</tr>
<tr>
<td>Web Application supports AD FS Claims Authentication</td>
<td>Selected</td>
</tr>
<tr>
<td>Url of the SharePoint AD FS Server</td>
<td>The URL of the ADFS server which is trusted by SharePoint.</td>
</tr>
<tr>
<td>Trust Identifier for SharePoint</td>
<td>The Relying Party Trust identifier for the SharePoint web application. [more]</td>
</tr>
<tr>
<td>Allow Complex Identities</td>
<td>Selected</td>
</tr>
</tbody>
</table>

**Notes:** You can configure the security provider to operate when multiple ADFS servers are used to authenticate users in SharePoint. [more]

5. Create a SharePoint security provider. [more]
Key parameter | Value
--- | ---
Name | You must name your security provider.
Security Provider Type | SharePoint
User Identity | The user identity you just created.
Active Directory Security Provider | The default Active Directory security provider.
Security Provider for SharePoint Users | The Claims for SharePoint On-Premises security provider you just created.
Security Provider for Domain Groups | (none)
SharePoint Server Url | The URL of the SharePoint web application where the Coveo SharePoint Web Service is installed in the form http://SharePoint_server:[WebApp_port].
AuthenticationType | AdfsUnderClaims
AdfsServerUrl | The URL of the ADFS server for which a Trust is established with SharePoint.
SharePointTrustIdentifier | The Relying Party Trust identifier for the SharePoint web application, such as urn:federation:MicrosoftOnline.[more]

Notes: You can configure the security provider to operate when multiple ADFS servers are used to authenticate users in SharePoint. [more]

6. Create a SharePoint or OneDrive for Business source.

Key parameter | SharePoint | OneDrive for Business
--- | --- | ---
Name | You must name your source. |  
Source Type | SharePoint (x64) | OneDrive for Business
Addresses | The URL for the SharePoint farm sections that you want to index in the form https://SharePoint_server[:port]/path, where [path] is needed only when you want index a specific site collection, list, etc. | The URL for the SharePoint web application that you want to index in the form https://SharePoint_server:[WebApp_port].
Authentication Type | AdfsUnderClaims |  

www.coveo.com
### Key parameter

<table>
<thead>
<tr>
<th>Key parameter</th>
<th>SharePoint</th>
<th>OneDrive for Business</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>AdfsServerUrl</strong></td>
<td>The URL of the ADFS server for which a trust is established with SharePoint.</td>
<td></td>
</tr>
<tr>
<td>(Hidden parameter)</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>SharePointTrustIdentifier</strong></td>
<td>The Relying Party Trust identifier for the SharePoint ADFS server. [more]</td>
<td></td>
</tr>
<tr>
<td>(Hidden parameter)</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Authentication</strong></td>
<td>The user identity you created.</td>
<td></td>
</tr>
<tr>
<td><strong>Security Provider</strong></td>
<td>The SharePoint Security provider you just created.</td>
<td></td>
</tr>
</tbody>
</table>

**Notes:** You can configure the source to operate when multiple ADFS servers are used to authenticate users in SharePoint.

7. Rebuild the source and validate that documents are indexed.

**What's Next?**

- (For SharePoint sources only) When you provide a Coveo .NET Front-End search interface residing outside SharePoint and want users to be able to find Claims-secured SharePoint content without having to log in again to SharePoint, configure the search interface to manage single sign-on.

- **CES 7.0.9093+ (September 2017)** (For SharePoint on-premises sources only) When you provide a Coveo JavaScript search interface and want to leverage SharePoint claims for content security, install the Coveo Claims Security Module, among other things (see "Allowing a JavaScript Search Page to Retrieve SharePoint Claims" on page 1316).

9.30.4.4 SharePoint 2016/2013/2010 On-Premises (Federated - Okta) Source Quick Setup

1. Validate that your environment meets the requirements:
   - **CES 7.0.9272+ (March 2018)**
     
     **Note:** You can check your CES version from the Administration Tool.
   
   - Your Coveo license includes the Microsoft SharePoint connector.

2. Create a user identity.
### Key parameter | Value
---|---
Name | You must name your user identity.
User | An Okta SSO recognized account in the `username@mydomain.com` form that can see all the content that you want to index.
Password | The corresponding password.

3. Ensure that the account of your user identity has the appropriate permissions:
   
a. For content and permission indexing, incremental refresh, and site collection discovery, the account must have Administrator permission for all SharePoint site collections to index, but also the root site collection.
   
   [more]

   b. For personal site and social tags indexing, the account must be owner of all personal sites collections
   
   [more].

   **Note:** User profiles cannot be crawled using a claim-based authentication (see Only Windows users can be added to Service Application security).

4. Create a Claims for SharePoint On-Premises security provider. [more]

### Key parameter | Value
---|---
Name | You must name your security provider (ex.: Claims SharePoint Okta).
Security Provider Type | Claims for SharePoint On-Premises
User Identity | (none)
SharePoint Web Application Url | In the form https://site:8080/
Temporary path for the cache of the User Claims | Enter a path of the folder in which the cache should be stored (ex.: C:\tmp)
Url of the SharePoint AD FS Server | Leave this box empty.
Trust Identifier for SharePoint | Leave this box empty.

5. Create a SharePoint security provider. [more]

### Key parameter | Value
---|---
Name | You must name your security provider (ex.: SharePoint Okta).
6. Create a SharePoint source.

<table>
<thead>
<tr>
<th>Key parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>You must name your source (ex.: Claims SharePoint Okta).</td>
</tr>
<tr>
<td>Source Type</td>
<td>SharePoint</td>
</tr>
<tr>
<td>Addresses</td>
<td>The SharePoint server URL in the form <a href="https://site:8080/%5Bpath">https://site:8080/[path</a>], where [path] is needed only when you want index a specific site collection, list, etc.</td>
</tr>
<tr>
<td>Crawling Scope</td>
<td>WebApplication</td>
</tr>
<tr>
<td>Authentication Type</td>
<td>Okta</td>
</tr>
<tr>
<td>Authentication</td>
<td>The user identity you created in step 2.</td>
</tr>
<tr>
<td>Security Provider</td>
<td>The SharePoint security provider you created in step 7.</td>
</tr>
</tbody>
</table>

7. Rebuild the source and validate that documents are indexed.

8. When a claims-aware Coveo Search is used, you can test the searchability of the source [more]
   
   a. Add the Claims for SharePoint security provider that you created in step 4 to the Coveo .NET Front-End search interface.
   
   b. Log in to the search interface with an Okta SSO recognized user, and then verify that you can see search
results from the source you created in step 6, but only documents to which this user has access in SharePoint.

9.30.4.5 SharePoint Online (Native) [Claims] Source Quick Setup

1. Validate that your environment meets the requirements:
   - **CES 7.0.6767+ (June 2014)**

   OR

   (For Microsoft OneDrive for Business) **CES 7.0.8047+ (December 2015)**

   **Note:** You can check your CES version from the Administration Tool.

   - Your Coveo license includes the Microsoft SharePoint or Microsoft OneDrive for Business connector.
   - **CES 7.0.8047+ (December 2015)** DNS records for Office 365 at your DNS hosting provider

2. Create a user identity with a dedicated Windows account that has access to all the SharePoint content that you want to index.

<table>
<thead>
<tr>
<th>Key parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Name</strong></td>
<td>You must name your user identity.</td>
</tr>
<tr>
<td><strong>User</strong></td>
<td>A native Office 365 account in the <code>username@domain.onmicrosoft.com</code> form</td>
</tr>
<tr>
<td><strong>Password</strong></td>
<td>The corresponding password.</td>
</tr>
</tbody>
</table>

3. Ensure that the Windows account of your user identity has the appropriate permissions:
   a. For content and permission indexing, incremental refresh, and site collection discovery, the account must have Administrator permission for all SharePoint Online site collections to index, but also the root site collection. [more]
b. For personal site, user profile, and social tags indexing, the account must be owner of all personal sites collections. [more]

4. Create a Claims for SharePoint Online security provider. [more]

<table>
<thead>
<tr>
<th>Key parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>You must name your security provider.</td>
</tr>
<tr>
<td>Security Provider Type</td>
<td>Claims for SharePoint Online</td>
</tr>
<tr>
<td>User Identity</td>
<td>The user identity you just created.</td>
</tr>
<tr>
<td>SharePoint Web Application Url</td>
<td>In the form <a href="https://domain.sharepoint.com">https://domain.sharepoint.com</a></td>
</tr>
<tr>
<td>Office 365 Native Users Domain(s)</td>
<td>In the form domain.onmicrosoft.com [more]</td>
</tr>
</tbody>
</table>

5. Install the Windows Azure AD module on the Coveo Master server needed by the Office 365 security provider. [more]

6. Create an Office 365 security provider. [more]

<table>
<thead>
<tr>
<th>Key parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>You must name your security provider.</td>
</tr>
<tr>
<td>Security Provider Type</td>
<td>Office 365</td>
</tr>
<tr>
<td>User Identity</td>
<td>The native Office 365 user identity you created.</td>
</tr>
<tr>
<td>Users Security Provider</td>
<td>The Claims for SharePoint Online security provider you just created.</td>
</tr>
</tbody>
</table>

7. Create a SharePoint security provider. [more]

<table>
<thead>
<tr>
<th>Key parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>You must name your security provider.</td>
</tr>
<tr>
<td>Security Provider Type</td>
<td>SharePoint</td>
</tr>
<tr>
<td>User Identity</td>
<td>The native Office 365 user identity you created.</td>
</tr>
<tr>
<td>Active Directory Security Provider</td>
<td>(none)</td>
</tr>
<tr>
<td>Security Provider for SharePoint Users</td>
<td>The Claims for SharePoint Online security provider you just created.</td>
</tr>
</tbody>
</table>
### Key parameter | Value
--- | ---
**Security Provider for Domain Groups** | The Office 365 security provider you just created.

**SharePoint Server URL** | URL of the SharePoint Online site in the form `https://domain.sharepoint.com/[path]` where `[path]` is needed only when you want index a specific site collection, list, etc.

**Authentication Type** | SpOnlineNative

---

8. Create a SharePoint or OneDrive for Business source.

<table>
<thead>
<tr>
<th>Key parameter</th>
<th>SharePoint</th>
<th>OneDrive for Business</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Name</strong></td>
<td>You must name your source.</td>
<td></td>
</tr>
<tr>
<td><strong>Source Type</strong></td>
<td>SharePoint (x64)</td>
<td>OneDrive for Business</td>
</tr>
</tbody>
</table>
| **Addresses** | The SharePoint Online server URL in the form `https://domain.SharePoint.com` | The URL of the SharePoint Online site collection regrouping all the personal sites (in which are located the OneDrives for Business) that you want to index in the form `https://domain-my.sharepoint.com`.

| **Authentication Type** | SpOnlineNative | |
| **Authentication** | The native Office 365 user identity you created. | |
| **Security Provider** | The SharePoint Security provider you just created. | |

9. Rebuild the source and validate that documents are indexed.

9.30.4.6 SharePoint Online (ADFS SSO) [Claims] Source Quick Setup
1. Validate that your environment meets the requirements:
   - CES 7.0.6767+ (June 2014)
   OR
   (For Microsoft OneDrive for Business) CES 7.0.8047+ (December 2015)
   
   **Note:** You can check your CES version from the Administration Tool.
   - Your Coveo license includes the Microsoft SharePoint or Microsoft OneDrive for Business connector.
   - Your ADFS setup meets Coveo requirements. [more]
   - CES 7.0.8047+ (December 2015) DNS records for Office 365 at your DNS hosting provider

2. Create a user identity with a dedicated account that has access to all the SharePoint content that you want to index.

<table>
<thead>
<tr>
<th>Key parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>You must name your user identity.</td>
</tr>
<tr>
<td>User</td>
<td>A single sign-on Office 365 account in the <code>username@domain.com</code> form.</td>
</tr>
<tr>
<td>Password</td>
<td>The corresponding password.</td>
</tr>
</tbody>
</table>

3. Ensure that the account of your user identity has the appropriate permissions:
   a. For content and permission indexing, incremental refresh, and site collection discovery, the account must have Administrator permission for all SharePoint Online site collections to index, but also the root site
collection. [more]

b. For personal site, user profile, and social tags indexing, the account must be owner of all personal sites collections. [more]

4. Create a Claims for SharePoint Online security provider. [more]

<table>
<thead>
<tr>
<th>Key parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>You must name your security provider.</td>
</tr>
<tr>
<td>Security Provider Type</td>
<td>Claims for SharePoint Online</td>
</tr>
<tr>
<td>User Identity</td>
<td>When a claims-aware Coveo Search is used, select a user identity of any Windows account that can be used to authenticate to ADFS. Otherwise, select the user identity you just created. [more]</td>
</tr>
<tr>
<td>SharePoint Web Application Url</td>
<td>In the form <a href="https://domain.sharepoint.com">https://domain.sharepoint.com</a></td>
</tr>
<tr>
<td>Office 365 Native Users Domain(s)</td>
<td>In the form domain.onmicrosoft.com[more]</td>
</tr>
<tr>
<td>Allow Complex Identities</td>
<td>Selected</td>
</tr>
</tbody>
</table>

Notes: You can configure the security provider to operate:

- When single sign-on is enabled in Office 365. [more]
- When multiple ADFS servers are used to authenticate users in SharePoint. [more]

5. Install the Windows Azure AD module on the Coveo Master server needed by the Office 365 security provider. [more]

6. Create an Office 365 security provider. [more]

<table>
<thead>
<tr>
<th>Key parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>You must name your security provider.</td>
</tr>
<tr>
<td>Security Provider Type</td>
<td>Office 365</td>
</tr>
<tr>
<td>User Identity</td>
<td>The single sign-on Office 365 user identity you created.</td>
</tr>
</tbody>
</table>
### 7. Create a SharePoint security provider. [more]

<table>
<thead>
<tr>
<th>Key parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Users Security Provider</strong></td>
<td>The Claims for SharePoint Online security provider you just created.</td>
</tr>
<tr>
<td><strong>Windows Azure Active Directory Module</strong></td>
<td>The installation path of the Microsoft Online Services Module for Windows PowerShell. [more]</td>
</tr>
<tr>
<td><strong>for Windows PowerShell</strong></td>
<td></td>
</tr>
</tbody>
</table>

### 8. Create a SharePoint or OneDrive for Business source.

<table>
<thead>
<tr>
<th>Key parameter</th>
<th><strong>SharePoint</strong></th>
<th><strong>OneDrive for Business</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Name</strong></td>
<td>You must name your source.</td>
<td></td>
</tr>
<tr>
<td><strong>Source Type</strong></td>
<td>SharePoint (x64)</td>
<td>OneDrive for Business</td>
</tr>
</tbody>
</table>
### Key parameter | SharePoint | OneDrive for Business
---|---|---
**Addresses** | The SharePoint Online server URL in the form https://domain.SharePoint.com. | The URL of the SharePoint Online site collection regrouping all the personal sites (in which are located the OneDrives for Business) that you want to index in the form https://domain-my.sharepoint.com.

**Authentication Type** | SpOnlineFederated |  
**AdfsServerUrl** (Hidden parameter) | The URL of the ADFS server for which a trust is established with SharePoint. |
**SharePointTrustIdentifier** (Hidden parameter) | The Relying Party Trust identifier for the SharePoint ADFS server. | [more] |
**Authentication** | The single sign-on Office 365 user identity you created. |  
**Security Provider** | The SharePoint security provider you just created. |  

**Notes:** You can configure the source to operate when multiple ADFS servers are used to authenticate users in SharePoint.

9. Rebuild the source and validate that documents are indexed.

9.30.4.7 SharePoint Online (Okta SSO) [Claims] Source Quick Setup

1. Validate that your environment meets the requirements:
   - **CES 7.0.6767+ (June 2014)**
     OR
Note: You can check your CES version from the Administration Tool.

- Your Coveo license includes the Microsoft SharePoint or Microsoft OneDrive for Business connector.
- CES 7.0.8047+ (December 2015) DNS records for Office 365 at your DNS hosting provider

2. Create a user identity.

<table>
<thead>
<tr>
<th>Key parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>You must name your user identity.</td>
</tr>
<tr>
<td>User</td>
<td>An Okta SSO recognized account in the \textit{<a href="mailto:username@mydomain.com">username@mydomain.com</a>} form that can see all the content that you want to index.</td>
</tr>
<tr>
<td>Password</td>
<td>The corresponding password.</td>
</tr>
</tbody>
</table>

3. Ensure that the account of your user identity has the appropriate permissions:

   a. For content and permission indexing, incremental refresh, and site collection discovery, the account must have Administrator permission for all SharePoint Online site collections to index, but also the root site collection. [more]

   b. For personal site, user profile, and social tags indexing, the account must be owner of all personal sites collections [more].

4. Create a Claims for SharePoint Online security provider. [more]

<table>
<thead>
<tr>
<th>Key parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>You must name your security provider (\textit{ex.: Claims SharePoint Online Okta}).</td>
</tr>
<tr>
<td>Security Provider Type</td>
<td>Claims for SharePoint Online</td>
</tr>
<tr>
<td>User Identity</td>
<td>The user identity you created in step 2.</td>
</tr>
<tr>
<td>SharePoint Web Application Url</td>
<td>In the form \textit{<a href="https://mydomain.sharepoint.com%7D">https://mydomain.sharepoint.com}</a></td>
</tr>
<tr>
<td>Office 365 Native Users Domain(s)</td>
<td>In the form \textit{mydomain.onmicrosoft.com}\textit{[more]}</td>
</tr>
<tr>
<td>Single Sign-On (AD FS) is enabled</td>
<td>Selected</td>
</tr>
</tbody>
</table>
### Key parameter | Value
--- | ---
**Url of the SharePoint AD FS Server** | The full path to your SharePoint Online ActiveClientSignInUrl that should be in the form: 
https://mydomain.okta.com/app/office365/[GUID]/sso/wsfed/active 
You can find your SharePoint Online ActiveClientSignInUrl in Okta, in the sign on instructions of the Microsoft Office 365 application: 
  a. With an administrator account, log in into Okta. 
  b. In the top menu, click **Admin**. 
  c. In the administration panel, select **Applications > Applications**. 
  d. In the **Applications** page, click **Microsoft Office 365**. 
  e. In the **Microsoft Office 365** page, select the **Sign On** tab. 
  f. In the **Sign On** tab, under **Sign On Methods** section, click **View Setup Instructions**. 
  g. The ActiveClientSignInUrl is the value next to **ActiveLogOnUri**. 

**Trust Identifier for SharePoint** | urn:federation:MicrosoftOnline

5. Install the Windows Azure AD module on the Coveo Master server needed by the Office 365 security provider [more].

6. Create an Office 365 security provider. [more]

### Key parameter | Value
--- | ---
**Name** | You must name your security provider (ex: Office 365 SharePoint Online Okta). 

**Security Provider Type** | Office 365 

**User Identity** | The user identity you created in step 2. 

**Users Security Provider** | The Claims for SharePoint Online security provider you just created. 

**Windows Azure Active Directory Module for Windows PowerShell** | The installation path of the Microsoft Online Services Module for Windows PowerShell.[more]

7. Create a SharePoint security provider. [more]

### Key parameter | Value
--- | ---
**Name** | You must name your security provider (ex: SharePoint Online Okta). 

**Security Provider Type** | SharePoint 

**User Identity** | The user identity you created in step 2.
### Key parameter | Value
--- | ---
Active Directory Security Provider | **Active Directory** to resolve AD users. *(none)* to only recognize Okta SSO users.
Security Provider for SharePoint Users | The **Claims for SharePoint Online** security provider you created in step 4.
Security Provider for Domain Groups | The **Office 365** security provider you just created in step 6.
SharePoint Server Url | URL of the SharePoint Online site in the form https://mydomain.sharepoint.com/[path], where [path] is needed only when you want index a specific site collection, list, etc.
AuthenticationType | SpOnlineFederated
AdfsServerUrl | The same path you entered when configuring the Claims for SharePoint Online security provider (see AdfsServerUrl).
SharePointTrustIdentifier | The Relying Party Trust identifier for the SharePoint web application, such as urn:federation:MicrosoftOnline.  
**[more]**

**Notes:** You can configure the security provider to operate when multiple ADFS servers are used to authenticate users in SharePoint.  
**[more]**

8. Create a SharePoint or OneDrive for Business source.

<table>
<thead>
<tr>
<th>Key parameter</th>
<th>SharePoint</th>
<th>OneDrive for Business</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>You must name your source <em>(ex.: Claims SharePoint Online Okta or Claims OneDrive for Business Okta).</em></td>
<td></td>
</tr>
<tr>
<td>Source Type</td>
<td>SharePoint (x64)</td>
<td>OneDrive for Business</td>
</tr>
<tr>
<td>Addresses</td>
<td>The SharePoint Online server URL in the form <a href="https://mydomain.SharePoint.com">https://mydomain.SharePoint.com</a>.</td>
<td>The URL of the SharePoint Online site collection regrouping all the personal sites (in which are located the OneDrives for Business) that you want to index in the form <a href="https://domain-my.sharepoint.com">https://domain-my.sharepoint.com</a>.</td>
</tr>
<tr>
<td>Crawling Scope</td>
<td>WebApplication</td>
<td>N/A</td>
</tr>
<tr>
<td>Authentication Type</td>
<td>SpOnlineFederated</td>
<td></td>
</tr>
<tr>
<td>AdfsServerUrl</td>
<td>(Hidden parameter)</td>
<td>The same path you entered when configuring the Claims for SharePoint Online security provider (see AdfsServerUrl).</td>
</tr>
</tbody>
</table>
### Key parameter

| SharePointTrustIdentifier (Hidden parameter) | The Relying Party Trust identifier for the SharePoint web application, such as urn:federation:MicrosoftOnline. [more] |
| Authentication | The user identity you created in step 2. |
| Security Provider | The SharePoint security provider you created in step 7. |

**Notes:** You can configure the source to operate when multiple ADFS servers are used to authenticate users in SharePoint.

9. Rebuild the source and validate that documents are indexed.

10. (Not for OneDrive for Business sources) When a claims-aware Coveo Search is used, you can test the searchability of the source [more]

   a. Add the Claims for SharePoint security provider that you created in step 4 to the Coveo .NET Front-End search interface.

   b. Log in to the search interface with an Okta SSO recognized user, and then verify that you can see search results from the source you created in step 8, but only documents to which this user has access in SharePoint Online.

9.30.4.8 SharePoint Online (Federated - Okta) [Email] Source Quick Setup

1. Validate that your environment meets the requirements:
   - CES 7.0.7433+ (February 2015)
   - OR
Your Coveo license includes the Microsoft SharePoint or Microsoft OneDrive for Business connector.

Your domain is federated (see Okta / Microsoft Office 365 Deployment Guide).

SharePoint user emails must match the one they use to log in to your Coveo search interface.

CES 7.0.8047+ (December 2015) DNS records for Office 365 at your DNS hosting provider

2. Create a user identity with a dedicated Windows account that has access to all the SharePoint content that you want to index.

<table>
<thead>
<tr>
<th>Key parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>You must name your user identity.</td>
</tr>
<tr>
<td>User</td>
<td>An Okta SSO recognized account in the <a href="mailto:username@domain.com">username@domain.com</a> form that can see all the content that you want to index.</td>
</tr>
<tr>
<td>Password</td>
<td>The corresponding password.</td>
</tr>
</tbody>
</table>

3. Ensure that the account of your user identity has the appropriate permissions:
   a. For content and permission indexing, incremental refresh, and site collection discovery, the account must have Administrator permission for all SharePoint Online site collections to index, but also the root site collection. [more]
   b. For personal site, user profile, and social tags indexing, the account must be owner of all personal sites collections. [more]

4. Create an Email security provider. [more]

<table>
<thead>
<tr>
<th>Key parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>You must name your security provider.</td>
</tr>
<tr>
<td>Security Provider Type</td>
<td>Email (x64)</td>
</tr>
<tr>
<td>User Identity</td>
<td>The federated Office 365 user identity you created.</td>
</tr>
</tbody>
</table>

5. Create a Claims to Email for SharePoint Online security provider.

<table>
<thead>
<tr>
<th>Key parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>You must name your security provider.</td>
</tr>
</tbody>
</table>
6. Install the Windows Azure AD module on the Coveo Master server needed by the Office 365 security provider. [more]

7. Create an Office 365 security provider. [more]

<table>
<thead>
<tr>
<th>Key parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security Provider Type</td>
<td>Claims to Email for SharePoint Online</td>
</tr>
<tr>
<td>User Identity</td>
<td>The federated Office 365 user identity you created.</td>
</tr>
<tr>
<td>Security Provider</td>
<td>The Email security provider you created in step 4.</td>
</tr>
<tr>
<td>Windows Azure Active Directory Module</td>
<td>The installation path of the Microsoft Online Services Module</td>
</tr>
<tr>
<td>for Windows PowerShell</td>
<td>for Windows PowerShell. [more]</td>
</tr>
</tbody>
</table>

8. Create a SharePoint security provider. [more]

<table>
<thead>
<tr>
<th>Key parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>You must name your security provider.</td>
</tr>
<tr>
<td>Security Provider Type</td>
<td>Office 365</td>
</tr>
<tr>
<td>User Identity</td>
<td>The federated Office 365 user identity you created.</td>
</tr>
<tr>
<td>Users Security Provider</td>
<td>The Claims to Email for SharePoint Online security provider you</td>
</tr>
<tr>
<td></td>
<td>just created.</td>
</tr>
<tr>
<td>Windows Azure Active Directory Module</td>
<td>The installation path of the Microsoft Online Services Module</td>
</tr>
<tr>
<td>for Windows PowerShell</td>
<td>for Windows PowerShell. [more]</td>
</tr>
<tr>
<td>Active Directory Security Provider</td>
<td>(none)</td>
</tr>
<tr>
<td>Security Provider for SharePoint Users</td>
<td>The Claims to Email for SharePoint Online security provider you</td>
</tr>
<tr>
<td></td>
<td>just created.</td>
</tr>
<tr>
<td>Security Provider for Domain Groups</td>
<td>The Office 365 security provider you just created.</td>
</tr>
</tbody>
</table>
### Key parameter | Value
--- | ---
**SharePoint Server Url** | URL of the SharePoint Online site in the form  
https://domain.sharepoint.com/[path]  
where [path] is needed only when you want index a specific site collection, list, etc.

**AuthenticationType** | SpOnlineFederated

**AdfsServerUrl** | The full path to your SharePoint Online ActiveClientSignInUrl that should be in the form:  
https://mydomain.okta.com/app/office365/[GUID]/sso/wsfed/active  
You can find your SharePoint Online ActiveClientSignInUrl in Okta, in the sign on instructions of the Microsoft Office 365 application:

a. With an administrator account, log in into Okta.
b. In the top menu, click Admin.
c. In the administration panel, select Applications > Applications.
d. In the Applications page, click Microsoft Office 365.
e. In the Microsoft Office 365 page, select the Sign On tab.
f. In the Sign On tab, under Sign On Methods section, click View Setup Instructions.
g. The ActiveClientSignInUrl is the value next to ActiveLogOnUri.

**SharePointTrustIdentifier** | The Relying Party Trust identifier for the SharePoint web application, such as urn:federation:MicrosoftOnline.

9. Create a SharePoint or OneDrive for Business source.

### Key parameter | SharePoint | OneDrive for Business
--- | --- | ---
**Name** | You must name your source (ex: Claims SharePoint Online Okta or Claims OneDrive for Business Okta). |  
**Source Type** | SharePoint (x64) | OneDrive for Business
**Addresses** | The SharePoint Online server URL in the form  
https://mydomain.SharePoint.com | The URL of the SharePoint Online site collection regrouping all the personal sites (in which are located the OneDrives for Business) that you want to index in the form  

**Crawling Scope** | WebApplication | N/A
**Authentication Type** | SpOnlineFederated |  
**AdfsServerUrl** (Hidden parameter) | The same path you entered when configuring the SharePoint security provider (see AdfsServerUrl). |  
**SharePointTrustIdentifier** (Hidden parameter) | The Relying Party Trust identifier for the SharePoint web application, such as urn:federation:MicrosoftOnline.
1. Validate that your environment meets the requirements:
   - CES 7.0.7433+ (February 2015)
     OR
   (For Microsoft OneDrive for Business) CES 7.0.8047+ (December 2015)
   
   **Note:** You can check your CES version from the Administration Tool.
   
   - Your Coveo license includes the Microsoft SharePoint or Microsoft OneDrive for Business connector.
   - Your ADFS setup meets Coveo requirements. [more]
   - SharePoint user emails must match the one they use to log in to your Coveo search interface.
   - CES 7.0.8047+ (December 2015) DNS records for Office 365 at your DNS hosting provider

2. Create a user identity with a dedicated Windows account that has access to all the SharePoint content that you want to index.
### Key parameter | Value
--- | ---
**Name** | You must name your user identity.
**User** | A single sign-on Office 365 account in the *username@domain.com* form.
**Password** | The corresponding password.

3. Ensure that the account of your user identity has the appropriate permissions:
   
a. For content and permission indexing, incremental refresh, and site collection discovery, the account must have Administrator permission for all SharePoint Online site collections to index, but also the root site collection. [more]
   
b. For personal site, user profile, and social tags indexing, the account must be owner of all personal sites collections. [more]

4. Create an Email security provider. [more]

<table>
<thead>
<tr>
<th>Key parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Name</strong></td>
<td>You must name your security provider.</td>
</tr>
<tr>
<td><strong>Security Provider Type</strong></td>
<td>Email (x64)</td>
</tr>
<tr>
<td><strong>User Identity</strong></td>
<td>The federated Office 365 user identity you created.</td>
</tr>
</tbody>
</table>

5. Create a Claims to Email for SharePoint Online security provider.

<table>
<thead>
<tr>
<th>Key parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Name</strong></td>
<td>You must name your security provider.</td>
</tr>
<tr>
<td><strong>Security Provider Type</strong></td>
<td>Claims to Email for SharePoint Online</td>
</tr>
<tr>
<td><strong>User Identity</strong></td>
<td>The federated Office 365 user identity you created.</td>
</tr>
<tr>
<td><strong>Security Provider</strong></td>
<td>The Email security provider you created in step 4.</td>
</tr>
<tr>
<td><strong>Windows Azure Active Directory Module for Windows PowerShell</strong></td>
<td>The installation path of the Microsoft Online Services Module for Windows PowerShell. [more]</td>
</tr>
</tbody>
</table>

6. Install the Windows Azure AD module on the Coveo Master server needed by the Office 365 security provider. [more]

7. Create an Office 365 security provider. [more]
### Key parameter | Value
--- | ---
Name | You must name your security provider.
Security Provider Type | Office 365
User Identity | The federated Office 365 user identity you created.
Users Security Provider | The [Claims to Email for SharePoint Online](#) security provider you just created.
Windows Azure Active Directory Module for Windows PowerShell | The installation path of the Microsoft Online Services Module for Windows PowerShell. [more]

8. Create a SharePoint security provider. [more]

### Key parameter | Value
--- | ---
Name | You must name your security provider.
Security Provider Type | SharePoint
User Identity | The federated Office 365 user identity you created.
Active Directory Security Provider | (none)
Security Provider for SharePoint Users | The [Claims to Email for SharePoint Online](#) security provider you just created.
Security Provider for Domain Groups | The Office 365 security provider you just created.
SharePoint Server Url | URL of the SharePoint Online site in the form https://domain.sharepoint.com/[path] where [path] is needed only when you want to index a specific site collection, list, etc.
AuthenticationType | SpOnlineFederated
AdfsServerUrl | The URL of the ADFS server for which a trust is established with SharePoint.
SharePointTrustIdentifier | The Relying Party Trust identifier for the SharePoint web application, such as urn:federation:MicrosoftOnline.[more]

9. Create a SharePoint or OneDrive for Business source.
### Key parameter | SharePoint (x64) | OneDrive for Business
--- | --- | ---
**Name** | You must name your source (ex.: Claims SharePoint Online ADFS or Claims OneDrive for Business ADFS). |  
**Source Type** | SharePoint (x64) | OneDrive for Business
**Addresses** | The SharePoint Online server URL in the form https://mydomain.SharePoint.com. | The URL of the SharePoint Online site collection regrouping all the personal sites (in which are located the OneDrives for Business) that you want to index in the form https://domain-my.sharepoint.com.

**Crawling Scope** | WebApplication | N/A

**Authentication Type** | SpOnlineFederated |  
**AdfsServerUrl** (Hidden parameter) | The URL of the ADFS server for which a trust is established with SharePoint. |  
**SharePointTrustIdentifier** (Hidden parameter) | The Relying Party Trust identifier for the SharePoint web application, such as urn:federation:MicrosoftOnline.[more] |  
**Authentication** | The user identity you created in step 2. |  
**Security Provider** | The SharePoint security provider you created in step 8. |  

10. Rebuild the source and validate that documents are indexed.

9.30.4.10 SharePoint Online (Native) [Email] Source Quick Setup
1. Validate that your environment meets the requirements:
   
   - [CES 7.0.6767+ (June 2014)](https://www.coveo.com)
   
   OR
   
   (For Microsoft OneDrive for Business) [CES 7.0.8047+ (December 2015)](https://www.coveo.com)
   
   **Note:** You can check your CES version from the Administration Tool.
   
   - Your Coveo license includes the Microsoft SharePoint or Microsoft OneDrive for Business connector.
   - [CES 7.0.8047+ (December 2015)](https://www.coveo.com) DNS records for Office 365 at your DNS hosting provider
   
2. Create a user identity with a dedicated Windows account that has access to all the SharePoint content that you want to index.

<table>
<thead>
<tr>
<th>Key parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>You must name your user identity.</td>
</tr>
<tr>
<td>User</td>
<td>A native Office 365 account.</td>
</tr>
<tr>
<td><strong>Note:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>- When you use your own domain in Office 365: <code>username@domain.com</code>.</td>
</tr>
<tr>
<td></td>
<td>- When you use the initial domain in Office 365: <code>username@domain.onmicrosoft.com</code>.</td>
</tr>
<tr>
<td>Password</td>
<td>The corresponding password.</td>
</tr>
</tbody>
</table>

3. Ensure that the Windows account of your user identity has the appropriate permissions:

   a. For content and permission indexing, incremental refresh, and site collection discovery, the account must have Administrator permission for all SharePoint Online site collections to index, but also the root site collection. [more]

   b. For personal site, user profile, and social tags indexing, the account must be owner of all personal sites collections. [more]

4. Create an Email security provider. [more]

<table>
<thead>
<tr>
<th>Key parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>You must name your security provider.</td>
</tr>
<tr>
<td>Security Provider Type</td>
<td>Email (x64)</td>
</tr>
<tr>
<td>User Identity</td>
<td>The federated Office 365 user identity you created.</td>
</tr>
</tbody>
</table>

5. Create a Claims to Email for SharePoint Online security provider.
<table>
<thead>
<tr>
<th>Key parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>You must name your security provider.</td>
</tr>
<tr>
<td>Security Provider Type</td>
<td>Claims to Email for SharePoint Online</td>
</tr>
<tr>
<td>User Identity</td>
<td>The federated Office 365 user identity you created.</td>
</tr>
<tr>
<td>Security Provider</td>
<td>The Email security provider you created in step 4.</td>
</tr>
<tr>
<td>Windows Azure Active Directory Module for Windows PowerShell</td>
<td>The installation path of the Microsoft Online Services Module for Windows PowerShell. [more]</td>
</tr>
</tbody>
</table>

6. Install the Windows Azure AD module on the Coveo Master server needed by the Office 365 security provider. [more]

7. Create an Office 365 security provider. [more]

<table>
<thead>
<tr>
<th>Key parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>You must name your security provider.</td>
</tr>
<tr>
<td>Security Provider Type</td>
<td>Office 365</td>
</tr>
<tr>
<td>User Identity</td>
<td>The native Office 365 user identity you created.</td>
</tr>
<tr>
<td>Users Security Provider</td>
<td>The Claims for SharePoint Online security provider you just created.</td>
</tr>
</tbody>
</table>

8. Create a SharePoint security provider. [more]

<table>
<thead>
<tr>
<th>Key parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>You must name your security provider.</td>
</tr>
<tr>
<td>Security Provider Type</td>
<td>SharePoint</td>
</tr>
<tr>
<td>User Identity</td>
<td>The native Office 365 user identity you created.</td>
</tr>
<tr>
<td>Active Directory Security Provider</td>
<td>(none)</td>
</tr>
<tr>
<td>Security Provider for SharePoint Users</td>
<td>The Claims to Email for SharePoint Online security provider you just created.</td>
</tr>
<tr>
<td>Security Provider for Domain Groups</td>
<td>The Office 365 security provider you just created.</td>
</tr>
</tbody>
</table>
## Coveo Platform 7.0 | Administrator Guide

### Key parameter | Value
--- | ---
**SharePoint Server Url** | URL of the SharePoint Online site in the form https://domain.sharepoint.com/[path] where [path] is needed only when you want index a specific site collection, list, etc.

**AuthenticationType** | SpOnlineNative

---

9. Create a SharePoint or OneDrive for Business source.

<table>
<thead>
<tr>
<th>Key parameter</th>
<th>SharePoint</th>
<th>OneDrive for Business</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Name</strong></td>
<td>You must name your source.</td>
<td></td>
</tr>
<tr>
<td><strong>Source Type</strong></td>
<td>SharePoint (x64)</td>
<td>OneDrive for Business</td>
</tr>
<tr>
<td><strong>Addresses</strong></td>
<td>The SharePoint Online server URL in the form <a href="https://domain.SharePoint.com">https://domain.SharePoint.com</a>.</td>
<td>The URL of the SharePoint Online site collection regrouping all the personal sites (in which are located the OneDrives for Business) that you want to index in the form <a href="https://domain-my.sharepoint.com">https://domain-my.sharepoint.com</a>.</td>
</tr>
<tr>
<td><strong>Authentication Type</strong></td>
<td>SpOnlineNative</td>
<td>N/A</td>
</tr>
<tr>
<td><strong>Authentication</strong></td>
<td>The native Office 365 user identity you created.</td>
<td></td>
</tr>
<tr>
<td><strong>Security Provider</strong></td>
<td>The SharePoint security provider you just created.</td>
<td></td>
</tr>
</tbody>
</table>

10. Rebuild the source and validate that documents are indexed.

### 9.30.5 Microsoft SharePoint Connector Deployment Overview

The following procedure outlines the steps needed to deploy the second generation Microsoft SharePoint connector. The SharePoint connector supports several SharePoint versions as well as various authentication modes. The configuration steps depend on the configuration of your SharePoint environment.

1. Validate that your environment meets the requirements:
   - Coveo license for the Microsoft SharePoint connector
     
     Your Coveo license must include support for the Microsoft SharePoint connector to be able to use this connector.
   - CES 7.0.8047+ (December 2015) (For SharePoint Online only) Configure DNS settings for Office 365 at your DNS hosting provider.
a. Log in to Office 365 admin center with an administrator account.

b. In the navigation bar on the left, select Setup, and then Domains.

c. In the Home > Domains page, under Domain Name, click your corporate domain (company.onmicrosoft.com).

d. In the [domain name] page, in the DNS settings section, take note of the DNS records.

e. Configure these DNS records in your DNS host provider (see Create DNS records at any DNS hosting provider for Office 365).

f. In the [domain name] page, in the DNS records section, click the Troubleshoot domain link to ensure the DNS records were correctly configured.

- CES 7.0.6767+ (June 2014)

- ADFS requirements
When your SharePoint environment uses ADFS as a trusted identity provider, your ADFS setup must meet specific requirements (see "ADFS Server Requirements for a Claims Security Provider" on page 1330).

- Okta requirements
When your SharePoint environment uses Okta as an SSO provider, your Okta setup must meet specific requirements (see Okta Single Sign-On Provider for SharePoint On-Premises).

- Supported SharePoint version:
  - SharePoint Online
  - CES 7.0.8541+ (September 2016) SharePoint 2016 (on-premises)
  - SharePoint 2013 (on-premises)
    - Microsoft SharePoint Foundation 2013
    - Microsoft SharePoint 2013 (SharePoint 2013)
  - SharePoint 2010 (on-premises)
    - Microsoft SharePoint Foundation 2010 (WSS 4)
    - Microsoft SharePoint 2010 (SharePoint 2010)

Notes:
- You can index on-premises SharePoint 2007 content with the SharePoint Legacy connector.
- Coveo Platform 7 does not support indexing SharePoint 2003 content.

2. Referring to the following table, identify the SharePoint environment type that you want to index (Classic, Claims, or Online type).
3. On your SharePoint farm (tenant in SharePoint Online):

   a. Select or create a user that the connector will use to crawl your SharePoint content. Refer to the following table to identify the required type of user for your type of SharePoint environment.

<table>
<thead>
<tr>
<th>SharePoint environment type</th>
<th>SharePoint Web Application Enabled authentication</th>
<th>Type of user</th>
<th>User format</th>
</tr>
</thead>
<tbody>
<tr>
<td>Classic (2010, 2013, or 2016)</td>
<td>Windows</td>
<td>Windows account</td>
<td>domain\username or <a href="mailto:username@domain.com">username@domain.com</a></td>
</tr>
<tr>
<td>Claims (2010, 2013, or 2016)</td>
<td>Windows</td>
<td>Windows account</td>
<td><a href="mailto:username@domain.com">username@domain.com</a></td>
</tr>
<tr>
<td></td>
<td>ADFS</td>
<td>ADFS SSO</td>
<td><a href="mailto:username@domain.com">username@domain.com</a></td>
</tr>
<tr>
<td>Okta</td>
<td>Okta SSO</td>
<td>user format</td>
<td><a href="mailto:username@domain.com">username@domain.com</a></td>
</tr>
<tr>
<td>Online</td>
<td>Native</td>
<td>Native Office 365 account</td>
<td><a href="mailto:username@domain.onmicrosoft.com">username@domain.onmicrosoft.com</a></td>
</tr>
<tr>
<td></td>
<td>SSO with ADFS</td>
<td>Single Sign-On Office 365 account</td>
<td><a href="mailto:username@domain.com">username@domain.com</a></td>
</tr>
<tr>
<td></td>
<td>SSO with Okta</td>
<td></td>
<td><a href="mailto:username@domain.com">username@domain.com</a></td>
</tr>
</tbody>
</table>

   b. For on-premises environments, install the Coveo web service, search box, and search interface on your SharePoint farm (see "Installing the Coveo Web Service, Search Box, and Search Interface into SharePoint" on page 1309).

   **Note:** With this installation procedure, you can also integrate the Coveo search box to SharePoint. Integrating the search box is not required to deploy the connector and it can be done later.
If you plan on creating a JavaScript search page and want to leverage claims from your on-premises SharePoint farm, you can install the Coveo Claims Security Module rather than the Coveo .NET Front-End web service (see "Coveo JavaScript Search Framework" on page 144 and "Allowing a JavaScript Search Page to Retrieve SharePoint Claims" on page 1316).

**Important**: Do not install both the Coveo Claims Security Module and the Coveo .NET Front-End web service, as this would create duplicate files on your server.

c. Grant appropriate SharePoint permissions to the crawling account you selected to ensure access to all the content that you want to index (see "Granting SharePoint Permissions to the Crawling Account" on page 1307).

d. **CES 7.0.8541+ (September 2016)** For on-premises environments, when you have thousands of user profiles in your farm, it is recommended to create a search service application to list your user profiles (see "Listing User Profiles With a SharePoint Search Service Application" on page 1283).

4. On the Coveo Master server, in the Administration Tool:

a. Configure the user identity

   Once the crawling account has been set up, you must create a CES user identity for this account.

b. When indexing SharePoint Online content, you must install the Windows Azure AD module on the Coveo Master server because it is needed by the Office 365 security provider (see "Installing the Windows Azure AD Module for Windows PowerShell" on page 1331).

c. Referring to the following table, create the security providers required for your SharePoint environment following the order in the numerical icons.

<table>
<thead>
<tr>
<th>Required security provider type</th>
<th>Online</th>
<th>2016/2013/2010 on-premises</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Office 365 Native</td>
<td>SSO ADFS</td>
</tr>
<tr>
<td>Active Directory</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Claims for SharePoint on-premises</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Claims for SharePoint Online</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>Claim to Email for SharePoint Online</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Office 365</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SharePoint</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

www.coveo.com
Note: When an Active Directory security provider is required, use the out-of-the-box Active Directory security provider.

d. CES 7.0.6607+ (April 2014) Create a SharePoint field set to take advantage of the metadata available on SharePoint content.

i. It is recommended to start by importing the default SharePoint field set file ([CES\Path]\Bin\Coveo.CES.CustomCrawlers.SharePoint.FieldSet.xml) to create fields for all the metadata available by default from SharePoint documents.

ii. When you created custom metadata for your SharePoint documents, add corresponding fields to the field set.

e. Configure and index the Microsoft SharePoint source

The Coveo connector needs to know details about your Microsoft SharePoint server or farm to be able to index its content (see "Configuring and Indexing a Microsoft SharePoint Source" on page 1292).

5. When you provide a Coveo .NET search interface residing outside SharePoint and want users to be able to find Claims-secured SharePoint content without having to log in again to SharePoint, configure the search interface to manage single sign-on (see "Manually Configuring a .NET Search Interface Claims SSO for an On-Premises SharePoint" on page 178).

9.30.6 Listing User Profiles With a SharePoint Search Service Application

CES 7.0.8541+ (September 2016) The Coveo connector for SharePoint supports to retrieve the user profiles directly from the SharePoint 2010, 2013, and 2016 search service application. This method is particularly useful for farms containing thousands of user profiles to improve the indexing performance.

Once the search service application has retrieved all user profiles, the Coveo connector queries the application for all profiles.

To list user profiles with a SharePoint search service application

1. With an administrator account, access the SharePoint Central Administration.

2. In the Central Administration page, click Manage service applications.

3. If you do not already have one, create a search service application:

   a. In the top menu, in the Create section, click the New drop-down list menu, and then select Search Service Application.

   b. In the Create New Search Service Application dialog:

      i. In the fist box, enter a meaningful Service Application Name.

         Example: Coveo Connector

      ii. Click OK.

4. In the application list, click the Name of the application.

5. In the [Search Service Application Name]: Search Administration page, in the menu on the left, under
Crawling, click Content Sources.

6. In the [Search Service Application Name]: Manage Content Sources page, click the Local SharePoint sites source Name.

7. In the [Search Service Application Name]: Edit Content Source page, in the Type start addresses below (one per line) box, cut the URL starting with sps3, and then click OK.

8. Back in the [Search Service Application Name]: Manage Content Sources page, click New Content Source.

9. In the [Search Service Application Name]: Add Content Source page:
   a. In the first box, enter a content source Name.
      
      Example: mysites host

   b. In the Type start addresses below (one per line) box, paste the URL that you cut in step 8.

   c. Under Full Crawl, click Create schedule.

      Note: The full crawl is necessary for the SharePoint connector to take account of deleted user profiles.

   d. In the Manage Schedules dialog:
      i. Next to Settings, in the Run every box, enter 1.

      ii. Next to Settings, in the Starting time drop-down list menu, select a time at least one hour prior the start of your SharePoint V2 source refresh (see Configuring and Indexing a Microsoft SharePoint Source).

      iii. Click OK.

   e. Click OK.

10. (For SharePoint 2013 and 2016 only) Back in the [Search Service Application Name]: Manage Content Sources page, in the menu on the left, under Queries and Results, click Result Sources.

11. (For SharePoint 2013 and 2016 only) In the [Search Service Application Name]: Manage Result Sources page, click Local People Results drop-down list menu, and then select Set as Default.

    Note: Setting the Local People Results result source as default allowed the application to return user profiles.

What's Next?

While configuring your SharePoint V2 source (see "Configuring and Indexing a Microsoft SharePoint Source" on page 1292), retrieve the list of user profiles from the native SharePoint Crawler, by adding the LoadUserProfiles and UsePeopleSearchForUserProfiles hidden parameters and set the parameter values to true.

9.30.7 Creating a SharePoint Security Provider

SharePoint and OneDrive for Business (CES 7.0.8047+ (December 2015)) sources need a SharePoint security provider to resolve permissions found on documents in the unified index. These permissions can either be SharePoint groups, users, or domain groups. Of these three types of permissions, only SharePoint groups are

www.coveo.com
actually processed by the SharePoint security provider. Users and domain groups are simply forwarded to other security providers for processing.

The other types of security providers required to process users and domain groups vary according to the SharePoint environment being indexed, more precisely, according to the type of authentication provider (Classic Windows, Claims-Based) used by the Web Application, and the SharePoint server version (2013 or 2010 on-premises, or Online).

Notes:

- CES 7.0.6830+ (July 2014) The SharePoint security provider type is for the second-generation SharePoint and the OneDrive for Business connectors. When you are still using the original SharePoint connector to create your SharePoint source, ensure to rather use the SharePoint Legacy security provider type.
- You can get familiar with how Coveo components deal with permissions on documents both at indexing and query time.

To modify or configure a SharePoint security provider

1. On the Coveo server, access the Administration Tool.
3. In the Security page, in the navigation panel on the left, click Security Providers.
5. In the Modify Security Provider page:
## Modify Security Provider

Modifies the parameters of the security provider.

### Security Providers

- **Name**
  - **SharePoint**

- **Security Provider Type**
  - **SharePoint Security Provider**

- **Description**
  - **SharePoint**

- **DLL Path**
  - **CoveoCES/SecurityProviders/SharePoint.dll**

- **User Identity**
  - **(none)**

- **Active Directory Security Provider**
  - **(none)**

### Security Provider for SharePoint Users

- **SharePoint Server URL**
- **Cache expiration delay (in minutes)**
- **Authentication Type**
  - **WindowsClassic**

### Security Provider for Domain Groups

- **Active Directory Security Provider**
  - **(none)**

### Parameters

- **Allow Basic Authentication**
- **Okta Realm**
- **Okta Sign In URL**

### Allow Complex Identities

- **Used By**
a. In the Name box, enter a name to identify this security provider.

Example: You may want to include in the name the SharePoint version and authentication mode used by this security provider:

SharePoint 2013 (Windows under Claims)

b. In the Security Provider Type drop-down list, select SharePoint (x64).

Note: CES 7.0.6767–(June 2014) The SharePoint (x64) type corresponds to what is now the Legacy SharePoint security provider.

c. In the User Identity section:

i. In the drop-down list, select the user identity that you selected or created previously to connect to this SharePoint Web Application.

ii. When needed, click Add, Edit, or Manage user identities respectively to create, modify, or manage user identities.

d. In the Active Directory Security Provider drop-down list:

i. For on-premises SharePoint environments without an Okta single sign-on configuration, select the default Active Directory security provider

ii. For SharePoint Online environments, select (none).

iii. For on-premises SharePoint environment using an Okta single sign-on configuration, select (none).

e. In the Security Provider for SharePoint Users drop-down list, select the security provider that you created for your SharePoint environment.

- Classic: Select (none).

- Claims or Okta: Select your Claims security provider for an on-premises SharePoint (see "Creating a Claims Security Provider for an On-Premises SharePoint" on page 1319).

- Online:

  ○ Select your Claims security provider for SharePoint Online (see "Creating a Claims Security Provider for SharePoint Online" on page 1326).

  OR

  ○ CES 7.0.7433+ (February 2015) Select your Claims to Email security provider for SharePoint Online (see "Creating a Claims to Email Security Provider for SharePoint Online" on page 1324).

f. In the Security Provider for Domain Groups drop-down list, select the security provider that you created for your SharePoint environment.

- Classic: Select (none).

- Claims (on-premises) or Okta: Select (none).
**g.** In the **SharePoint Server Url** box, enter the following value according to your SharePoint environment:

- **Classic**: URL of the SharePoint Web Application where the secured content to index is located.
- **Claims (on-premises) or Okta**: URL of the SharePoint Web Application to index where the Coveo SharePoint Web Service is installed in the form `http://SharePoint_server[:WebApp_port].`

**Note:** You can find the port of the Coveo Web Service on your SharePoint server (see **How to: Identify the Port Number of a SharePoint Application**).

- **Online**: URL of the SharePoint online site in the form `https://domain.sharepoint.com/[path].`

**h.** In the **Cache expiration delay (in minutes)** box, you can set the time interval at which the security provider cache is refreshed. The default and recommended value is 60 minutes.

**Example:** You may want to significantly reduce the **Cache expiration delay (in minutes)** value to 1 minute while you perform permission changing tests and want to ensure that this cache does not significantly delay the effect of your permission changes. You would set the value back to the default when your tests are completed to optimize performances.

**i.** In the **Authentication Type** box, refer to the following table to enter the authentication type value corresponding to your SharePoint environment and the type of **User Identity** that you assigned to this security provider.

<table>
<thead>
<tr>
<th>SharePoint environment</th>
<th>User identity type</th>
<th>Value to enter</th>
</tr>
</thead>
<tbody>
<tr>
<td>Classic</td>
<td>Windows account (SharePoint 2010 default)</td>
<td>WindowsClassic</td>
</tr>
<tr>
<td></td>
<td>ADFS federated account</td>
<td>AdfsUnderClaims</td>
</tr>
<tr>
<td></td>
<td>Okta</td>
<td>Okta</td>
</tr>
<tr>
<td>Online</td>
<td>Native Office 365 account</td>
<td>SpOnlineNative</td>
</tr>
<tr>
<td></td>
<td>Single Sign-On Office 365 account</td>
<td>SpOnlineFederated</td>
</tr>
</tbody>
</table>

**j.** Leave the **AuthenticationRealmUrl** box empty unless your SharePoint environment includes an online authentication service on a separate server, in which case you enter the authentication server URL.

**k.** The following ADFS related parameters are only required when the **Authentication Type** is either AdfsUnderClaims or SpOnlineFederated.
i. In the `AdfsServerUrl` box, enter the URL of the ADFS server for which a Trust is established with SharePoint.

   **Example:** https://adfs.mydomain.com

   **Note:** CES 7.0.6684+ (May 2014) The SharePoint connector supports indexing SharePoint online configured with Okta.

   In this case, in the `AdfsServerUrl` box, enter the full path to your SharePoint Online `ActiveClientSignInUrl` that should be in the form:

   https://acme.okta.com/app/office365/abcdefghGWUMNWLWYGXF/sso/wsfed/active

   You can find your SharePoint Online `ActiveClientSignInUrl` in Okta, in the sign on instructions of the Microsoft Office 365 application:

   i. With an administrator account, log in into Okta.

   ii. In the top menu, click **Admin**.

   iii. In the administration panel, select **Applications > Applications**.

   iv. In the **Applications** page, click **Microsoft Office 365**.

   v. In the **Microsoft Office 365** page, select the **Sign On** tab.

   vi. In the **Sign On** tab, under **Sign On Methods** section, click **View Setup Instructions**.

   vii. The `ActiveClientSignInUrl` is the value next to `ActiveLogOnUri`.

   Ensure that you also set this `ActiveClientSignInUrl` for the Claims Security provider and the SharePoint source (see Creating a Claims Security Provider for SharePoint Online).

ii. In the `SharePointTrustIdentifier` box, enter the Relying Party Trust identifier for the SharePoint web application (see "Finding the Relying Party Trust Identifier for a SharePoint Web Application" on page 111).

l. The following parameters are required only when multiple ADFS servers are used to authenticate users in SharePoint:

   i. In the `IdentityProviderServerUrl` box, enter the URL of the ADFS server which is used as an Identity Provider for the ADFS server trusted by SharePoint.

   ii. In the `AdfsServerTrustIdentifier` box, enter the Relying Party Trust identifier for the SharePoint ADFS server (see "Finding the Relying Party Trust Identifier for a SharePoint ADFS server" on page 112).

   **Note:** At this point, the proper ADFS endpoint(s) should already have been enabled on the ADFS server(s) during the configuration of the Claims security provider for SharePoint (see "ADFS Server Requirements for a Claims Security Provider" on page 1330).

m. Select the `AllowBasicAuthentication` option only when basic authentication is enabled on the web application to index and specifically want to use this authentication mode.
It is recommended to use this authentication method only with a secured connection (HTTPS) because the user name and password are passed in clear text in the URL.

n. **CES 7.0.9272+ (March 2018)** If your SharePoint instance uses an Okta single sign-on setup, in the **OktaRealm** box, enter the $realm value obtained from Okta (see "Retrieve your application parameters" on page 1306).

   **Example**: urn:okta:sharepoint:myid

o. **CES 7.0.9272+ (March 2018)** If your SharePoint instance uses an Okta single sign-on setup, in the **OktaSignInUrl** box, enter the $signInURL value you obtained from Okta (see "Retrieve your application parameters" on page 1306).

   **Example**: https://YOURINSTANCE_OKTA_OR_OKTAPREVIEW.com/app/sharepoint_onpremise/sso/wsfed/passive

p. In the **Parameters** section, in rare cases the Coveo Support could instruct you to click **Add Parameters** to specify other security provider parameter names and values that could help to troubleshoot security provider issues.

q. Leave the **Allow Complex Identities** option cleared as it does not apply to this type of security provider.

6. Click **Apply Changes**.

What's Next?

- (For SharePoint sources only) Configure and index a Microsoft SharePoint source.
- (For OneDrive for Business sources only) Configure and index a Microsoft OneDrive for Business source.

### 9.30.8 Creating and Using a Custom SharePoint Mapping File

A mapping file associates SharePoint metadata with Coveo index fields. SharePoint is essentially made of lists and list items. Each list has a **Base List Type**, to represent what it contains and how to interact with it.

**Example:** A Document Library list contains only documents. You can also add a Custom List which will contain generic list items. A user can have two Document Library lists, but decide to add more columns (metadata) to the second list.

**CES 7.0.6607+ (April 2014)** The Microsoft SharePoint connector comes with a default mapping file ([CES_Path]\bin\Coveo.CES.CustomCrawlers.SharePoint.MappingFile.xml) that contains mappings for all standard list types. Using the default mapping file allows to index standard SharePoint content.

While the content of custom metadata such as custom columns in a list are mapped to default fields, in a case where you identify custom metadata that are not properly mapped, you can consider creating and using a custom mapping file to ensure that custom metadata content is mapped to specific fields.
**Note:** In a custom SharePoint mapping file, you must refer to the custom SharePoint fields using the name that begins with the out-of-the-box `ows_` (Office Web Server) namespace prefix (see What does “ows” means and why people use it before name of a field).

You may identify a SharePoint metadata name from the SharePoint URL (see “Determining the Name of a SharePoint Metadata Tag” on page 522).

The SharePoint connector can put multiple mapping types in the `MappingType` property for every item, separated by semicolons, before being sent to the index.

These mapping types are arranged in order of more to less specific:

- Item type + ID (a GUID)
- Item type + Title
- Item type + Base type

**Example:** An item of a Contact list can have the following `MappingType`:

```
ListItem.{432-112324343-343331};ListItem.My Contact List;ListItem.Contacts
```

Items other than List and List Items have their ID and name:

```
Web.{58943-43849273-483922};Web.MyWeb
```

For all documents, the `DocumentType` property is set to the base item type (for example: `ListItem`).

Consequently, as shown in the following example, a mapping file can specifically map a set of lists or a single list to a particular set of fields.

**Important:** Semicolons (;) are used to separate items in the mapping file. When you want to map an item that has a ; character in its title, remove the character in the `MappingType` property (`<Mapping type="[Item title]">`).

```
<?xml version="1.0" encoding="utf-8"?>
<Mappings xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  xmlns:xsd="http://www.w3.org/2001/XMLSchema">
  <Version>1</Version>
  <CommonMapping>
    <Fields />
  </CommonMapping>
  ...
  <Mapping type="ListItem.Announcements">
    <Title>%[coveo_SiteName] - %[Title]</Title>
    <Body>%[Description]</Body>
    <Fields />
  </Mapping>
  <Mapping type="ListItem.GenericList.My custom list">
    <Title>%[coveo_SiteName] - %[Title]</Title>
    <Body>%[Description]</Body>
    <Fields>
      <Field name="myfield1">%{ows_customTextColumn1}</Field>
      <Field name="myfield2">%{ows_customTextColumn2}</Field>
      <Field name="myfield3">%{ows_customTextColumn3}</Field>
    </Fields>
  </Mapping>
</Mappings>
```
To create a custom SharePoint mapping file

1. Using an administrator account, connect to the Coveo Master server.

2. Copy the default mapping file ([CES_Path]\bin\Coveo.CES.CustomCrawlers.SharePoint.MappingFile.xml) and rename the copy in a folder under [Index_Path]\Config to ensure the file is part of your index configuration.

   **Example:** When your index is on the D: drive and you are indexing your SharePoint 2013 intranet, rename the copy of the default mapping file to:

   D:\CES70\Config\Connectors\SharePoint2013IntranetMapping.xml

3. Using a text editor, modify existing mappings or add new ones to specifically map your custom metadata.

   **Note:** The SharePoint mapping file must respect the standard mapping file schema (see "Standard Mapping File Schema" on page 58).

What's Next?

- In the source, ensure to select the custom mapping file you created (see Configuring and Indexing a Microsoft SharePoint Source).

- If you added custom fields, ensure to add them to the field set used by the source (see Microsoft SharePoint Connector Deployment Overview).

9.30.9 Configuring and Indexing a Microsoft SharePoint Source

A source defines a set of configuration parameters to extract and index Microsoft SharePoint content. This topic describes how to create a source using the second generation SharePoint connector.
Notes:

- In an environment with more than one Microsoft SharePoint Web Application, it is recommended to define one source for each Microsoft SharePoint Web Application that you want to index, and only index user profiles once to not create duplicates in your index (see Modifying Hidden Microsoft SharePoint Source Parameters).

- **CES 7.0.6830+ (July 2014)** The SharePoint source type is for the second generation SharePoint connector. When you are still using the original SharePoint connector to create your SharePoint source, ensure to rather use the SharePoint Legacy source type.

To configure and index a Microsoft SharePoint source

1. On the Coveo server, access the Administration Tool.
2. Select Index > Sources and Collections.
3. In the Collections section:
   a. Select an existing collection in which you want to add the new source.
   OR
   b. Click Add to create a new collection.
4. In the Sources section, click Add.
   
   The Add Source page that appears is organized in three sections.
5. In the General Settings section of the Add Source page:
a. Enter the appropriate value for the following required parameters:

**Name**

Enter a descriptive name of your choice for this source.

**Example:** When you have more than one SharePoint site to index, you can include in the name information to help distinguish between them.

SharePoint 2016 Intranet

SharePoint 2013 Extranet

**Source Type**

The connector used by this source. In this case, select **SharePoint**.

**Note:** CES 7.0.6767–(June 2014) The SharePoint type corresponds to what is now the Legacy SharePoint source type.

**Addresses**

List of specific SharePoint farm sections that you want to index. If you need to index more than one section, enter one URL per line.

**Note:** CES 7.0.6942 (August 2014) Starting addresses must end with /.
Examples:

- For the whole farm:
  `https://farm/`
- For a specific Web Application:
  `https://farm:8080/`
- For a specific site collection:
  `https://farm:8080/sites/Support/default.aspx`
- For a specific website:
- For a specific document library:
  `https://farm:8080/Document Library/
- For a specific list:
  `https://farm:8080/sites/Support/Lists/Contacts/AllItems.aspx`

**Important:** A specific folder in a list is not supported.

- For SharePoint Online:
  `https://domain.sharepoint.com`

**Note:** You can also use the source **Crawl Scope** parameter to control more precisely the content to crawl (see below).

**Fields**

Select the field set that you created for this source (see Microsoft SharePoint Connector Deployment Overview).

**Refresh Schedule**

Time interval at which the source is automatically refreshed to keep the index content up-to-date.

**Note:** The default **Every Day** option is typically good, but when your SharePoint content changes frequently within a day, after creating your source, you should schedule incremental refresh at significantly shorter time interval to continuously index ongoing SharePoint content changes. You can then consider to refresh the source weekly by selecting the **Every Sunday** option.

b. Review the value for the following parameters that often do not need to be modified:

**Rating**

Change this value only when you want to globally change the rating associated with all items in this source relative to the rating to other sources.
Example: If this source was for a legacy Intranet, you may want to set this parameter to Low, so that in the search interface, results from this source appear later in the list compared to those from other sources.

Document Types

If you defined custom document type sets, ensure to select the most appropriate for this source.

Active Languages

If you defined custom active language sets, ensure to select the most appropriate for this source.

6. In the Specific Connector Parameters & Options section of the Add Source page, review if you need to change the parameter default values:

   a. In the Number of Refresh Threads box, when your Coveo server has available CPU cores, consider increasing the number to easily and significantly increase the crawling performance. The default value is 2.

   b. In the Mapping File box, leave the default value to use the default mapping file (Coveo.CES.CustomCrawlers.SharePoint.MappingFile.xml).

      When you identify that some custom SharePoint content is not indexed or not properly mapped, consider creating a custom mapping file, and then enter the full path to the file (see "Creating and Using a Custom SharePoint Mapping File" on page 1290).

   c. CES 7.0.6830+ (July 2014) In the Crawling Scope drop-down box, select the option for the content type that you want to crawl in relation with the source Addresses that you specified (see above).

      Select WebApplication, the default value and highest element type in the SharePoint farm (tenant in SharePoint Online) hierarchy to crawl everything.
d. In the **Authentication Type** drop-down list, refer to the following table to select the authentication type value corresponding to your SharePoint environment and the type of **User Identity** that you assigned to this source (see Microsoft SharePoint Connector Deployment Overview).

<table>
<thead>
<tr>
<th>SharePoint environment</th>
<th>User identity type</th>
<th>Option to select</th>
</tr>
</thead>
<tbody>
<tr>
<td>Classic</td>
<td>Windows account (SharePoint 2010 default)</td>
<td>WindowsClassic</td>
</tr>
<tr>
<td>Claims</td>
<td>Windows account (SharePoint 2013 and 2016 default)</td>
<td>WindowsUnderClaims</td>
</tr>
<tr>
<td></td>
<td>ADFS federated account</td>
<td>AdfsUnderClaims</td>
</tr>
<tr>
<td></td>
<td>CES 7.0.9272+ (March 2018)</td>
<td>Okta</td>
</tr>
<tr>
<td>Online</td>
<td>Native Office 365 account</td>
<td>SpOnlineNative</td>
</tr>
<tr>
<td></td>
<td>Single Sign-On Office 365 account</td>
<td>SpOnlineFederated</td>
</tr>
</tbody>
</table>

e. In the **Parameters** section, click **Add Parameter** when you want to show and configure advanced hidden source parameters (see "Modifying Hidden Microsoft SharePoint Source Parameters" on page 1300).
Examples:

- In the case of an ADFS environment, when the **Authentication Type** parameter value is either `AdfsUnderClaims` or `SpOnlineFederated`, you must add ADFS related hidden parameters (see "ADFS Related Parameters" on page 1300).

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>AdfsServerUrl</td>
<td><a href="https://MyADFS2012.domain.com/">https://MyADFS2012.domain.com/</a></td>
</tr>
<tr>
<td>SharePointTrustIdentifier</td>
<td>urn:Federation:MicrosoftOnline</td>
</tr>
</tbody>
</table>

**Notes:** You can configure the security provider to operate when multiple ADFS servers are used to authenticate users in SharePoint. [more]

- **CES 7.0.8541+ (September 2016)** When you create a SharePoint search service application to list your user profiles, you must add the following hidden parameters (see `LoadUserProfiles` and `UsePeopleSearchForUserProfiles`).

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>LoadUserProfiles</td>
<td>true</td>
</tr>
<tr>
<td>UsePeopleSearchForUserProfiles</td>
<td>true</td>
</tr>
</tbody>
</table>

- **CES 7.0.9272+ (March 2018)** When your SharePoint instance uses Okta as a single sign-on provider, you must add the `OktaRealm` and `OktaSignInUrl` parameters, and the corresponding values that you previously retrieved (see Okta Single Sign-On Provider for SharePoint On-Premises).

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>OktaRealm</td>
<td>urn:okta:sharepoint:okta:01:vet:5t50h7</td>
</tr>
<tr>
<td>OktaSignInUrl</td>
<td><a href="https://10-154-158.okta">https://10-154-158.okta</a> preview.com/app/ sharepoint_onpremises/so/signed/passive</td>
</tr>
</tbody>
</table>

f. In the **Option** section:

**Index Subfolders**

Keep this check box selected (recommended). By doing so, all subfolders from the specified server address are indexed.

**Index the document's metadata**

When selected, CES indexes all the document metadata, even metadata that are not associated with a field. The orphan metadata are added to the body of the document so that they can be searched using free text queries.
When cleared (default), only the values of system and custom fields that have the Free Text Queries attribute selected will be searchable without using a field query.

**Example:** A document has two metadata:
- LastEditedBy containing the value Hector Smith
- Department containing the value RH

In CES, the custom field CorpDepartment is bound to the metadata Department and its Free Text Queries attribute is selected.

When the Index the document's metadata option is cleared, searching for RH returns the document because a field is indexing this value. Searching for hector does not return the document because no field is indexing this value.

When the Index the document's metadata option is selected, searching for hector also returns the document because CES indexed orphan metadata.

**Document's addresses are case-sensitive**

Leave the check box cleared. This parameter needs to be checked only in rare cases for case sensitive systems in which distinct documents may have the same file name but with different casing.

**Generate a cached HTML version of indexed documents**

When you select this check box (recommended), at indexing time, CES creates HTML versions of indexed documents. In the search interfaces, users can then more rapidly review the content by clicking the Quick View link rather than opening the original document with the original application. Consider clearing this check box only if you do not want to use Quick View links.

**Open results with cached version**

Leave this check box cleared (recommended) so that in the search interfaces, the main search result link opens the original document with the original application. Consider selecting this check box only when you do not want users to be able to open the original document but only see the HTML version of the document as a Quick View. In this case, you must also select Generate a cached HTML version of indexed documents.

7. In the Security section of the Add Source page:
a. In the **Authentication** drop-down list, select the user identity that you created for the Microsoft SharePoint farm (tenant in SharePoint Online) (see Microsoft SharePoint Connector Deployment Overview).

b. In the **Security Provider** drop-down list, select the SharePoint security provider that you created for this SharePoint source.

c. Click **Save** to save the source configuration and consider revising advanced source parameters before starting indexing the new source (see "Modifying Hidden Microsoft SharePoint Source Parameters" on page 1300).

OR

d. Click **Save and Start** to save and start indexing immediately.

**Note:** When your SharePoint Web Application uses Claims, the first time the SharePoint search interface is accessed, the first time setup page appears to let you enter your Claims information and allow access to the search interface (see Coveo .NET Front-End First Time Setup).

What’s Next?

Set an incremental refresh schedule for your source.

9.30.9.1 Modifying Hidden Microsoft SharePoint Source Parameters

The **Add Source** and **Source: ... General** pages of the Administration Tool present the parameters with which you can configure the connector for most Microsoft SharePoint setups. More advanced and more rarely used parameters are hidden. You can choose to make one or more of these parameters appear in the **Add Source** and **Source: ... General** pages of the Administration Tool so that you can change their default value.

The following list describes the available advanced hidden parameters for Microsoft SharePoint sources. The parameter type (integer, string…) appears between parentheses following the parameter name.

9.30.9.1.1 ADFS Related Parameters

The following ADFS related parameters are only required when the source **Authentication Type** parameter is either **AdfsUnderClaims** or **SpOnlineFederated**:

**AdfsServerUrl** (String)

URL of the AD FS server for which a trust is established with SharePoint.
The SharePoint connector supports indexing SharePoint Online configured with Okta (see "SharePoint Online (Okta SSO) [Claims] Source Quick Setup" on page 1265).

In this case, you must add the AdfsServerUrl hidden parameter to the source and set the value to the full path to your SharePoint Online ActiveClientSignInUrl that should be in the form:

https://acme.okta.com/app/office365/abcdefgGWUMNWLYGXF/sso/wsfed/active

You can find your SharePoint Online ActiveClientSignInUrl in Okta, in the sign on instructions of the Microsoft Office 365 application:

1. With an administrator account, log in to Okta.
2. In the top menu, click Admin.
3. In the administration panel, select Applications > Applications.
4. In the Applications page, click Microsoft Office 365.
5. In the Microsoft Office 365 page, select the Sign On tab.
6. In the Sign On tab, under Sign On Methods section, click View Setup Instructions.
7. The ActiveClientSignInUrl is the value next to ActiveLogOnUri.

Ensure that you also set this ActiveClientSignInUrl for the Claims Security provider and the SharePoint source (see Creating a Claims Security Provider for SharePoint Online and Creating a SharePoint Security Provider).

**SharePointTrustIdentifier (String)**

The Relying Party Trust identifier for the SharePoint ADFS server (see "Finding the Relying Party Trust Identifier for a SharePoint ADFS server" on page 112).

The following parameters are required only when multiple ADFS servers are used to authenticate users in SharePoint:

**IdentityProviderServerUrl (String)**

The URL of the ADFS server which is used as an Identity Provider for the ADFS server trusted by SharePoint.

**AdfsServerTrustIdentifier (String)**

Trust Identifier for the SharePoint AD FS Server. Enter the Relying Party Trust identifier for the SharePoint web application (see "Finding the Relying Party Trust Identifier for a SharePoint Web Application" on page 111).

9.30.9.1.2 Other Parameters

**UsePeopleSearchForUserProfiles (Boolean)** CES 7.0.8541+ (September 2016)

Note: User profiles are not available in Microsoft SharePoint Foundation.

Whether to extract the SharePoint user profiles using the SharePoint search service application (see "Listing User Profiles With a SharePoint Search Service Application" on page 1283). The default value is false.
When you have created a search service application, set this parameter to `true` only on the SharePoint source of your smallest web application in size.

You must also set the `LoadUserProfiles` hidden parameter to `true` (see `LoadUserProfiles`). Otherwise, the parameter is ineffective.

**AllowBasicAuthentication (Boolean)**

Select the `AllowBasicAuthentication` option only when basic authentication is enabled on the web application to index and specifically want to use this authentication mode. The default value is `false`.

It is recommended to use this authentication method only with a secured connection (HTTPS) because the user name and password are passed in clear text in the URL.

**AuthenticationRealmUrl (String)**

Add this hidden parameter only when your SharePoint environment includes an online authentication service on a separate server, in which case you enter the authentication server URL in the form `https://domain.sharepoint.com`.

**EnableOfficeIntegration (Boolean) [CES 7.0.7022+ (September 2014)]**

Whether to enable the office integration in the .NET UI or not. This will change the clickable URI to open documents directly in Office. The default value is `true`.

**LoadAllOnlineSiteCollections (Boolean) [CES 7.0.6830+ (July 2014)]**

Whether to extract the SharePoint Online site collections. The default value is `false`.

**LoadUserProfiles (Boolean)**

Whether to extract the SharePoint user profiles. The default value is `true`.

Set this parameter to `false` when you do not want to index the SharePoint users.
Notes:

- **CES 7.0.8541+ (September 2016)** Indexing user profiles takes a significantly smaller amount of time using the parameter in combination with the `UsePeopleSearchForUserProfiles` parameter (see `UsePeopleSearchForUserProfiles`).

- **CES 7.0.8388+ (June 2016)** Indexing user profiles can take a significant time depending on their number. Moreover, indexing user profiles more than once, creates as many duplicates in your index. It is thus recommended to only index your user profiles once for all your SharePoint sources:
  - When you configure your first SharePoint source, you do not need to add this parameter. For all your other SharePoint sources, add the `LoadUserProfiles` parameter and set the value to `false`.
  - When you already have other configured SharePoint source(s), look for your smallest Web Application in size, and add the `LoadUserProfiles` parameter and set the value to `false` in all your other SharePoint sources.

- Since SharePoint 2010, 2013 and 2016 do not support ADFS users on Windows with user profile, it is currently impossible when indexing those SharePoint versions to set the `LoadUserProfiles` parameter to `true` when the Crawl Scope is `WebApplication` and the Authentication Type is `AdfsUnderClaims` (see "Configuring and Indexing a Microsoft SharePoint Source" on page 1292).

- User profiles and personal websites are not available in Microsoft SharePoint Foundation.

### LoadSocialTags (Boolean) CES 7.0.7022+ (September 2014)

Whether to retrieve the social tags for each document or not. When set to `true`, documents corresponding to items with social tags have the fields `sysSptagNames` and `sysSptagGuids` set with the social tag content.

The parameter works for SharePoint On-Premises, but not for SharePoint Online. An incremental refresh should pick social tag changes. However, the SharePoint API does not report social tags accurately for all item types and the SharePoint web service cache can delay or cause multiple pick ups of a tag change by an incremental refresh.

The default value is `false`. Setting this parameter to `true` can have a significant impact on crawling performance because one call is required to retrieve each item.

### OverrideSharePointAuthor (Boolean) CES 7.0.7711+ (June 2015)

Whether to override the author saved in SharePoint for a document by the author extracted from the metadata of the document.

### RequestTimeout (Integer) CES 7.0.7711+ (June 2015)

The maximum amount of time (in seconds) an HTTP request can be executed before being canceled. The default value is `60`.

### WebPartsOptions (String) CES 7.0.7022+ (September 2014)

- **Note:** Not all Web parts are available in Microsoft SharePoint Foundation 2010 (see Overview of Web Parts available in SharePoint Foundation 2010).
Determines what to do with Web Part Pages. The content of the web parts is added to the field `syssearchablemeta`, which is not displayed in search results, but is searchable. Use this parameter to control what is indexed and include or not potentially secured dynamic content to prevent a security hole.

The following table lists the possible `WebPartsOptions` parameter values.

<table>
<thead>
<tr>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SelectiveWebParts</td>
<td>The default value. Only indexes the content of Web Parts listed in the</td>
</tr>
<tr>
<td></td>
<td><code>IncludedWebPartTypes</code> parameter.</td>
</tr>
<tr>
<td></td>
<td>By default, only fixed content is indexed, not dynamic content for which</td>
</tr>
<tr>
<td></td>
<td>permissions cannot be indexed and could potentially allow users to find</td>
</tr>
<tr>
<td></td>
<td>content to which they do not normally have access.</td>
</tr>
<tr>
<td>AllContent</td>
<td>Indexes the whole Web Part Page, including menus and dynamic web parts that</td>
</tr>
<tr>
<td></td>
<td>can contain secured content that will be searchable.</td>
</tr>
<tr>
<td>WebPartsContent</td>
<td>Indexes only the content of all the Web Parts of the Web Part Page, including</td>
</tr>
<tr>
<td></td>
<td>dynamic web parts that can contain secured content that will be searchable.</td>
</tr>
<tr>
<td>NoContent</td>
<td>Do not download and index the Web Part Page at all (indexed by reference).</td>
</tr>
</tbody>
</table>

Your mapping file should contain the following tags to ensure that the `syssearchablemeta` field gets set:

```xml
<Mapping type="File">
    <Fields>
        <Field name="syssearchablemeta">%coveo_AllMetaData</Field>
    </Fields>
</Mapping>
```

---

**IncludedWebPartTypes (String)** [CES 7.0.7022+ (September 2014)]

A semi-colon list of web part types to crawl for Web Part Pages when the `WebPartsOptions` parameter is set to `SelectiveWebParts`. By default only content editors are crawled (Microsoft.SharePoint.WebPartPages.ContentEditorWebPart;

**IndexListFolders (Boolean)** [CES 7.0.7104+ (October 2014)]

Whether to index List Folders or not. The default value is `false`, because Web folders are not accessible via the browser, only from Windows Explorer. Set to `true` when you want to see the List Folders in search results.

**ServerNameAlias (String)** [CES 7.0.7711+ (June 2015)]

Specifies a server name that overrides the one from which documents are downloaded in the index. This parameter is useful to have query results point to a server other than the one used for indexing.

**Example:** Three network load balanced (NLB) SharePoint front-end servers handle the end-users requests and your source crawls a fourth mirror server to not impact performance for users. In this case, you add the `ServerNameAlias` parameter and set the value to the NLB URL to replace the IP address in the index.
LoadPersonalSites (Boolean) CES 7.0.8047+ (December 2015)

Note: Personal websites are not available in Microsoft SharePoint Foundation.

When the Crawling Scope source parameter is set to WebApplication, whether to include personal sites. The default value is true.

OktaRealm (String) CES 7.0.9272+ (March 2018)

If your SharePoint instance uses an Okta single sign-on setup, provide the $realm value obtained from Okta (see "Retrieve your application parameters" on page 1306).

OktaSingInUrl (String) CES 7.0.9272+ (March 2018)

If your SharePoint instance uses an Okta single sign-on setup, provide the $signInURL value obtained from Okta (see "Retrieve your application parameters" on page 1306).

To modify hidden Microsoft SharePoint source parameters

1. Refer to "Adding an Explicit Connector Parameter" on page 450 to add one or more Microsoft SharePoint hidden source parameters.

2. For a new Microsoft SharePoint source, access the Add Source page of the Administration Tool to modify the value of the newly added advanced parameter:
   a. Select Index > Sources and Collections.
   b. Under Collections, select the collection in which you want to add the source.
   c. Under Sources, click Add.
   d. In the Add Source page, edit the newly added advanced parameter value.

3. For an existing Microsoft SharePoint source, access the Source: ... General page of the Administration Tool to modify the value of the newly added advanced parameter:
   a. Select Index > Sources and Collections.
   b. Under Collections, select the collection containing the source you want to modify.
   c. Under Sources, click the existing Microsoft SharePoint source in which you want to modify the newly added advanced parameter.
   d. In the Source: ... General page, edit the newly added advanced parameter value.

9.30.10 Okta Single Sign-On Provider for SharePoint On-Premises

SharePoint can use Okta as a trusted single sign-on (SSO) provider. Configure your Okta application and retrieve the application parameters so that the Coveo Claims security provider can authenticate users in SharePoint via Okta (see "Microsoft SharePoint Connector" on page 1243).

Requirements

- CES 7.0.9272+ (March 2018)
- SharePoint 2016, 2013, or 2010
You must add a trusted origin to the Okta application you use with your SharePoint instance:

1. Log in to your Okta Developer account.
2. Click Admin.
3. Click Security, and then, in the drop-down menu, select API.
4. Click the Trusted Origins tab.
5. In the Trusted Origins tab, click Add Origin.
6. In the Add Origin panel that appears:
   a. Under Name, enter a name.
      
      Example: Coveo Enterprise Search RedirectURI
   c. Select the Redirect checkbox.
   d. Click Save.

Retrieve your application parameters

Before you create a SharePoint security provider and source, you must retrieve two application parameters from Okta, as these parameters are required in the security provider and source configuration (see "Creating a SharePoint Security Provider" on page 1284 and "Configuring and Indexing a Microsoft SharePoint Source" on page 1292).

1. Log in to your Okta Developer account.
2. Click Admin.
3. Click Applications, and then, in the drop-down menu, select Applications.
4. Click the SharePoint (On-Premise) application linked to the SharePoint instance you want to make searchable.
5. Click Sign On.
7. In the new page that appears, under Setup a new authentication provider > Create the Okta Trusted Token issuer using PowerShell Script, take note of the $realm and $signInURL values, which should respectively be formatted as follows:

   Example:
   
   - urn:okta:sharepoint:myid
   - https://YOURINSTANCE_OKTA_OR_OKTAPREVIEW.com/app/sharepoint_onpremise/sso/wsfed/passive
These values are required when creating your SharePoint security provider and SharePoint source (see "Creating a SharePoint Security Provider" on page 1284 and "Configuring and Indexing a Microsoft SharePoint Source" on page 1292).

What's Next?

Create a SharePoint security provider (see "Creating a SharePoint Security Provider" on page 1284).

9.31 Microsoft SharePoint Connectors - Shared Topics

This section regroups topics applicable to both the "Microsoft SharePoint Connector" on page 1243 and the "Microsoft SharePoint Legacy Connector" on page 1334.

9.31.1 Granting SharePoint Permissions to the Crawling Account

You must select an existing account or create a new one that the SharePoint, SharePoint Legacy or OneDrive for Business (CES 7.0.8047+ (December 2015)) connector will use to crawl your SharePoint or OneDrive for Business content.

Tip: The best practice is to create a dedicated account for the exclusive use of the Coveo connector with a password that never changes. If you must change the password of this account you will need to change it both in the original identity provider system (AD or other) and in the corresponding CES user identity.

This crawling account must have the proper rights to retrieve the information from your SharePoint farm (tenant in SharePoint Online). There are two methods to configure the necessary SharePoint permissions for the crawling account.

- "Automatic Permissions Setup" on page 1307
- "Manual Permissions Setup" on page 1307

9.31.1.1 Automatic Permissions Setup

The SharePoint and SharePoint Legacy connectors have the ability to automatically set the required permissions to allow the crawling account to gain read access to the whole content as long as the following requirements are met:

- The Coveo SharePoint web service must be installed on the SharePoint farm (see "Installing the Coveo Web Service, Search Box, and Search Interface into SharePoint" on page 1309)

The crawling account must:

- Be a member of the SharePoint farm administrators group (see "Adding the Crawling Account to the SharePoint Farm Administrators Group" on page 105)
- Have the Read permission for the site collection(s) that you want to index (see "Adding the SharePoint Website Read Permission" on page 101).

9.31.1.2 Manual Permissions Setup

When your SharePoint environment does not meet the requirements for the automatic method, you must manually set permissions for your SharePoint crawling account.
The following table presents the minimal required permissions that the crawling account must have to perform the specified action for the supported SharePoint versions.

**Note:** CES 7.0.8047+ (December 2015) For OneDrive for Business, follow the actions applicable to your SharePoint version.

<table>
<thead>
<tr>
<th>SharePoint version</th>
<th>Action to perform</th>
<th>Minimal required permission</th>
</tr>
</thead>
<tbody>
<tr>
<td>Online</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2016</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>2013</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2010</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2007</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
| ✓                  | Content and Security indexing, incremental refresh, and site collection discovery | • CES 7.0.8047+ (December 2015) (Only when you index the content of a SharePoint web application) SharePoint Administrator permission in Office 365 (see Assigning admin roles in Office 365).  
  • Administrator permission for all SharePoint Online site collections, including the root site collection (see "Granting the Site Collection Administrator Permission in SharePoint Online" on page 113).  
  • Full Read policy for all SharePoint farm web applications (see "Adding the Full Read Policy to All SharePoint Farm Web Applications" on page 99). |
<p>| ✓                  |                   |                             |
| ✓                  |                   |                             |
| ✓                  |                   |                             |
| ✓                  |                   |                             |</p>
<table>
<thead>
<tr>
<th>SharePoint version</th>
<th>Action to perform</th>
<th>Minimal required permission</th>
</tr>
</thead>
<tbody>
<tr>
<td>Online 2016 2013 2010 2007</td>
<td>✓ ✓ ✓ ✓</td>
<td>Personal site, user profile and social tags indexing</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Notes:</strong></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• When indexing personal sites or user profiles, the crawling account must not have a personal site on the SharePoint server being indexed to prevent connector failure cases when attempting to retrieve the list of personal sites.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Personal sites and user profiles are not included in SharePoint Foundation.</td>
</tr>
<tr>
<td>✓ ✓ ✓ ✓</td>
<td></td>
<td><strong>Read</strong> permission for the site collection of the source starting address (see &quot;Adding the SharePoint Website Read Permission&quot; on page 101).</td>
</tr>
<tr>
<td>✓ ✓ ✓ ✓</td>
<td></td>
<td><strong>Retrieve People Data for Search Crawlers</strong> permission to the <strong>User Profile Service Application</strong> (see &quot;Adding the Retrieve People Data for Search Crawlers Permission to the User Profile Service Application&quot; on page 103).</td>
</tr>
<tr>
<td>✓ ✓ ✓ ✓</td>
<td></td>
<td><strong>Manage user profiles</strong> permission to the <strong>Shared Service Rights</strong> (see &quot;Adding the Manage User Profiles Permission in Shared Service Rights&quot; on page 105).</td>
</tr>
<tr>
<td>✓ ✓ ✓ ✓</td>
<td></td>
<td><strong>Owner of all personal sites collections</strong> (see &quot;Adding the Personal Sites Collections Owner Permissions for SharePoint Online&quot; on page 113).</td>
</tr>
</tbody>
</table>

**What's Next?**

Once you granted the appropriate permissions:

- (For SharePoint on-premises versions only) Optionally install the Coveo SharePoint web service (see "Installing the Coveo Web Service, Search Box, and Search Interface into SharePoint" on page 1309).

- (For SharePoint sources only) Create and index a SharePoint source.

- (For OneDrive for Business sources only) Create and index a OneDrive for Business source.

**9.31.2 Installing the Coveo Web Service, Search Box, and Search Interface into SharePoint**

The Coveo.NET Front-End can be integrated to an on-premises SharePoint by installing the following Coveo SharePoint web service, the Coveo search box, and the Coveo search interfaces components on all your SharePoint front-end servers.
If you plan on creating a JavaScript search page and want to leverage claims from your on-premises SharePoint farm, you can install the Coveo Claims Security Module rather than the Coveo .NET Front-End web service (see "Allowing a JavaScript Search Page to Retrieve SharePoint Claims" on page 1316).

**Important:** Do not install both the Coveo Claims Security Module and the Coveo .NET Front-End web service, as this would create duplicate files on your server.

**Coveo SharePoint web service**

The optional Coveo SharePoint web service installed on a SharePoint server enhances the Coveo SharePoint, SharePoint Legacy and OneDrive for Business (in a SharePoint 2013 or 2016 scenario) connectors ability to extract and index SharePoint content by providing:

- Full site collections discovery of the targeted SharePoint farms
- Automatic crawling account configuration (see "Automatic Permissions Setup" on page 1307)
- Possibility for end-users to log with SharePoint credentials in a Coveo search interface deployed outside of your SharePoint farm so that they can see SharePoint search results.

**Note:** Coveo .NET Front-End 12.0.99+ (March 2013) The Coveo SharePoint web service is optional only when all the content is indexed from a Classic SharePoint environment.

When indexing content from Web Applications using Claims-based Authentication Providers, the web service must be installed on the SharePoint server in order to add the following new features required by the Coveo Back-End and Mirror servers to handle Claims permissions:

- Convert permissions found on SharePoint document into Claims.
- Retrieve the list of Claims associated to a user performing a search in CES.

**Coveo search box**

You can also install the control for the Coveo search box on a SharePoint server and use it to replace the default SharePoint search box to get the benefits of the Coveo search results directly within SharePoint, providing another convenient Coveo access point.

**Note:** Installing the Coveo search box on the SharePoint server is optional and is not needed to deploy the Coveo SharePoint, SharePoint Legacy or OneDrive for Business (in a SharePoint 2013 or 2016 scenario) connector.
**Tip:** When the Coveo search box is installed on the SharePoint server, from the Interface Editor you can activate the **Enable search as you type** option in your SharePoint search interfaces to get quick search results directly under the search box. Note that you must install the **Default Search Interface** to gain access to the Interface Editor.

![Search Results Example](image)

**Coveo search interfaces**

When you choose to install the Coveo search box on your SharePoint server, you must also install Coveo search interfaces on the SharePoint server to present search results for queries performed from the Coveo search box.

**Tip:** You can configure the scope of each search interface using the Interface Editor.

**Important:** You must perform the following installation procedure for each web front-end server of your SharePoint farm, one after the other. You may see the **An update conflict has occurred, and you must re-try this action.** error message when installing concurrently on more than one server. You must also repeat this procedure each time you update or migrate the Coveo Platform on your Coveo Master server.

To install the Coveo SharePoint web service, search box, and search interface

1. Using a local administrator account, connect to the web front-end server of your SharePoint farm.

2. Ensure that the account you are using has the permissions presented in the following table.
3. Run the Coveo .NET Front-End installer.

4. When a required version of Microsoft Chart Controls for Dotnet Framework is missing on the server, in the dialog box that appears, click Install.

5. When a required version of Microsoft .NET Framework is missing on the server, in the dialog box that appears, click Install.

   Note: The Microsoft components are installed through the Internet. When the installer does not have access to the Internet, prerequisite installations will fail. You must then install the components manually and restart the Coveo .NET Front-End installer.

6. In the installer welcome screen, click Next.

7. In the installer License Agreement screen, read the license terms, select I accept the terms in the license
agreement, and then click Next.

8. In the Installing Folders screen:

![Installing Folders screen](image)

   a. For each optional item in the list, click the dropdown arrow and then ensure This feature will be installed on local hard drive. is selected for those that you want to install:

   - **Search Interface** - To install the search interface libraries used to handle search queries.
   - **Default Search Interface** - To install the default Coveo Enterprise Search web application and gain access to the Interface Editor.
     
     **Note:** When the Default Search Interface is not installed, you may get the The resource cannot be found error message when trying to access the Interface Editor from the search interface menu (Do more > Edit this interface).
     
   - **SharePoint Web Service** - Needed to allow the connector to automatically set permissions for the crawling account and to discover all site collections in the SharePoint farm.
   - **SharePoint Search Interface** - Needed when you want to integrate the Coveo SharePoint search interface in your SharePoint site.
   - **Coveo Search Box** - Needed when you want to replace the default SharePoint search box by the Coveo search box.
Tip: Once installed on your SharePoint server, you can enable/disable the Coveo search box independently for each site (see "Activating or Deactivating the Coveo .NET Search Box in a SharePoint Site" on page 176).

b. Click Next.

9. When you install the search interface and the search box, in the Configuration screen:

   a. Click Configure next to Web site hosting the interfaces.

   b. In the Web Interface Configuration screen:

      i. In the Web site name box, enter the name of the site to be created in IIS to host Coveo search interfaces.

      ii. In the Web site port box, enter the port to access the Coveo search interfaces. The default is 8080.

      iii. Click OK.

   c. Back in the Configuration screen, click Configure next to Coveo Enterprise Search server and port.

   d. In the CES Configuration screen:
i. In the **Server name** box, enter the hostname of the Coveo Back-End server (where CES is installed) to which you want to connect this Front-End server. You can leave `localhost` when CES is also installed on the current server.

ii. In the **Service port** box, change the CES service port default (52810) only when needed.

iii. Click **Test Server** to validate that the CES service is responding and compatible with the Coveo .NET Front-End you are installing.

iv. In the dialog box that appears, review the message to validation is successful, and then click **OK**.

v. Back in the **CES Configuration** screen, click **OK**.

e. Click **Next**.
10. In the installer **Installing the program** screen, click **Install**.

**Coveo .NET Front-End 12.0.1548+ (June 2016)** In a SharePoint farm with multiple Web Front-End (WFE) servers, you must install or update the Coveo .NET Front-End on each server. You can however speed up the installation by performing the changes to the SharePoint database only from the first server.

11. In the installer **Installation Successful** screen, click **Finish**.

What's Next?

- When you install the Coveo Front-End for the first time on a server, before you can use the search interfaces, you must link the Coveo Front-End to a Coveo Back-End server. In this case, the Coveo .NET Front-End installer automatically opens the **Front-End Server Configuration** page (see "Coveo .NET Front-End First Time Setup" on page 47).

- Create the appropriate security provider.

9.31.3 Allowing a JavaScript Search Page to Retrieve SharePoint Claims

**CES 7.0.8093+ (September 2017)**

When configuring a Coveo JavaScript search page, you may want to retrieve and leverage claims from your on-premises SharePoint instance (see "Coveo JavaScript Search Framework" on page 144). To do so, you must add a `SearchApiClaims.aspx` page to your SharePoint instance. Rather than adding it by installing the whole Coveo .NET Front-End web service, you can use a smaller installation kit to install the `SearchApiClaims.aspx` page only (see "Coveo SharePoint web service" on page 1310).

**Important:**

- You must perform the following installation procedure for each web front-end server of your SharePoint farm, one after the other. You may see the update conflict has occurred, and you must re-try this action. error message when installing concurrently on more than one server. You must also repeat this procedure each time you update or migrate the Coveo Platform on your Coveo Master server.

- Do not install both the Coveo Claims Security Module and the Coveo .NET Front-End web service, as this would create duplicate files on your server.

To allow a JavaScript search page to retrieve SharePoint claims

1. Using a local administrator account, connect to the web front-end server of your SharePoint farm.

2. Ensure that the account you are using has the permissions presented in the following table.

<table>
<thead>
<tr>
<th>SharePoint version</th>
<th>Required permissions</th>
</tr>
</thead>
<tbody>
<tr>
<td>2016/2013/2010</td>
<td>✓</td>
</tr>
<tr>
<td>2007</td>
<td>✓</td>
</tr>
</tbody>
</table>

Member of the SharePoint server local **Administrators** group (see "Adding the Crawling Account to the SharePoint Server Local Administrators Group" on page 118)
3. Download and run the Coveo Claims Security Module install kit (see Coveo Product Updates).

4. In the Coveo Claims Security Module 1.0 Installation dialog box that appears, proceed with the module installation:

   a. In the Welcome to Coveo Claims Security Module 1.0 screen, click Next.
   
   b. In the License Agreement screen, select I accept terms in the license agreement, and then click Next.
c. In the **Installing the program** screen, click **Install** to begin the module installation.

d. In the **Installation Successful** screen, click **Finish** to close the Coveo Claims Security Module install kit.
5. Edit the web.config file for your SharePoint site to complete installation, and then test your setup.

6. If not already done, create the appropriate security provider.

9.31.4 Creating a Claims Security Provider for an On-Premises SharePoint

When indexing content from a SharePoint Web Application using Claims-based authentication, the default in SharePoint 2013, you must create a Claims security provider to allow authenticated users to search for documents secured using Claims permissions. Without such a security provider, no results would be returned.

The role of the Claims security provider is to authenticate users in SharePoint and to retrieve the list of Claims associated to each user. Knowing the Claims of a user, the Coveo index can return the search results this user is entitled to see according to the permissions that were indexed on SharePoint documents.

In order to be authenticated by the Claims security provider, a user must log in to the Coveo search interface using his SharePoint credentials. The Claims security provider can authenticate users in SharePoint using a Windows identity or an identity provided by an Active Directory Federation Services (ADFS) server.
Notes:

- Coveo .NET Front-End version 12.0.99+ (March 2013 monthly release) is required to display search results with Claims permissions.

- The SharePoint, SharePoint Legacy and OneDrive for Business (CES 7.0.8047+ (December 2015)) connectors can use the Claims for SharePoint On-premises security provider type.

- You can get familiar with how Coveo components deal with permissions on documents both at indexing and query time.

To create a Claims security provider for an on-premises SharePoint

1. On the Coveo server, access the Administration Tool.

2. In the Administration Tool, select Configuration > Security.

3. In the navigation panel on the left, select Security Providers.


5. In the Modify Security Provider …:
a. In the **Name** box, enter a descriptive name of your choice for this security provider instance.

b. In the **Security Provider Type** drop-down, select **Claims for SharePoint On-premises**.

c. In the **User Identity** drop-down list:
   - In the case of an ADFS environment, when you select the **Web Application supports AD FS Claims Authentication** check box (see below) and a claims-aware Coveo Search is used (see "Configuring the Claims-Aware Coveo Search Application" on page 183), select a user identity of any Windows account that can be used to authenticate to ADFS.
   - Otherwise, select the user identity that you created for the Microsoft SharePoint farm.

d. In the **SharePoint Web Application Url** box, enter the URL of the SharePoint Web Application using
Claims-based authentication where the secured content to index is located.

e. In the **Temporary path for the cache of User Claims** box, you must enter the path where the temporary cache of user Claims is saved.

f. Select the **Web Application supports NTLM Claims Authentication** and/or **Web Application supports AD FS Claims Authentication** check boxes, according to the Claims authentication type that is enabled for the SharePoint web application (see “Finding the Enabled Claims Authentication Type for a SharePoint Web Application” on page 110).

**Important**: When using ADFS Claims Authentication, you need to make sure your ADFS environment meets the requirement for the Claims security provider (see "ADFS Server Requirements for a Claims Security Provider" on page 1330).

**Notes:**

- The Claims security provider can simultaneously support more than one Claims authentication type enabled for a Web Application.
- Select **Web Application supports NTLM Claims Authentication** for Windows authentication with NTLM or Kerberos.

g. **CES 7.0.5556+ (June 2013)** The following parameters are required only when the **Web Application supports AD FS Claims Authentication** check box is selected:

i. In the **Url of the SharePoint AD FS Server** box, enter the URL of the ADFS server which is trusted by SharePoint.

**Note**: If your SharePoint instance uses Okta as a single sign-on provider, leave this box empty (see “Okta Single Sign-On Provider for SharePoint On-Premises” on page 1305).

ii. In the **Trust Identifier for SharePoint** box, enter the Relying Party Trust identifier for the SharePoint web application (see "Finding the Relying Party Trust Identifier for a SharePoint Web Application" on page 111).

**Note**: If your SharePoint instance uses Okta as a single sign-on provider, leave this box empty (see “Okta Single Sign-On Provider for SharePoint On-Premises” on page 1305).

h. **CES 7.0.5556+ (June 2013)** The following parameters are required only when the **Web Application supports AD FS Claims Authentication** check box is selected and multiple ADFS servers are used to authenticate users in SharePoint:

i. In the **Url of the Identity Provider AD FS Server** box, enter the URL of the ADFS server which is used as an Identity Provider for the ADFS server trusted by SharePoint.

ii. In the **Trust Identifier for the SharePoint AD FS Server** box, enter the Relying Party Trust identifier for the SharePoint ADFS server (see "Finding the Relying Party Trust Identifier for a SharePoint ADFS server" on page 112).

i. **CES 7.0.5785+ (August 2013)** When the **Web Application supports AD FS Claims Authentication** check box is selected and a claims-aware Coveo Search is used (see “Configuring the Claims-Aware Coveo
Search Application" on page 183), in the **Bootstrap Token Signing Certificate (.cer)** box, enter the path on the Coveo Master server where you saved the certificate used by ADFS to sign requests from the claims-aware Coveo search. If the requests are not signed by ADFS, leave this parameter empty. If the requests are not signed by ADFS, leave this parameter empty.

j. In the **Claim Type for User Names** box, enter the type of Claim that should be used to uniquely identify users. Leave the default value (http://schemas.xmlsoap.org/ws/2005/05/identity/claims/nameidentifier) unless Coveo Support recommends to change the value.

k. In the **Claim Type(s) to Ignore** box, enter the type(s) of Claims that should be ignored by the security provider to prevent polluting the security cache with unnecessary claims.

Some of the Claims that are retrieved by the security provider when authenticating users in SharePoint can safely be ignored. These are usually Claims that are reserved for internal use by SharePoint and that cannot be used to set permissions on documents.

**Example:** SharePoint assigns to every user a Claim that identifies the last time the user was authenticated. The value of this Claim is a timestamp, which has no value regarding document permissions and cannot be selected in the SharePoint people picker.

l. **CES 7.0.9167+ (December 2017)** Select the **Expand user’s Granted Identities before first query** check box to evaluate users' granted identities before they perform their first query.

**Note:** When selected, results are returned following a user's first query. When cleared, results appear only after the user performs a second query or after the user's granted identities are expanded.

m. In the **Authentication Cookies Sliding Session Expiration Time (in days)** box, enter the time interval, in days, during which the Claims of a user authenticated by the Claims security provider remains valid. Values smaller than one day are accepted (ex.: 0.5). The default is 1 day.

n. Next to **Parameters**, when instructed to do so by Coveo Support, click **Add Parameter** to add an hidden parameter by entering the parameter **Name** and **Value**.

**Note:** **CES 7.0.6830+ (July 2014)** The parameter **ClaimsMaximumSize** is used to set the maximum allowed size for a single Claims identity. The default value is 12288 (12 KB). A message similar to the following one appears in the CES Console and logs typically when a user with claims exceeding this limit logged in or performed a query:

The security provider "Claims" has encountered an exception: class CSP::SecurityException: The user 'user_name here' contains too much claims and will be rejected.

When this condition occurs, the search results that are secured by Claims permissions are not returned for the query.

o. Ensure that the **Allow Complex Identities** option is selected.

A Claims security provider may need additional parameters when you create identities. You can specify these additional parameters only when the **Allow Complex Identities** option is selected.

p. **Click Save** or **Apply Changes**.
What's Next?

Create a SharePoint security provider that will use this Claims security provider.

9.31.5 Creating a Claims to Email Security Provider for SharePoint Online

You can get SharePoint Online users (native and federated) and Office 365 groups expanded to email users. A claims-based identity includes an email that the Claims to Email for SharePoint Online security provider extracts to resolve the identity of the user.

This security provider is useful either when you want to convert a claims identity to an email identity, or when you simply did not want to use a claims identity. The only requirement for the claims to email conversion to work is that the email your users enter to log in to SharePoint Online must match the email they use when logging into your Coveo search interface. The Claims to Email for SharePoint Online security provider was specifically designed for cloud environments where the identity is neither Claims nor Active Directory.

Notes:

- The SharePoint, SharePoint Legacy, and OneDrive for Business connectors can use the Claims to Email for SharePoint security provider type.
- You can get familiar with how Coveo components deal with permissions on documents both at indexing and query time.

To create a Claims to Email security provider for SharePoint Online

1. On the Coveo server, access the Administration Tool.
2. In the Administration Tool, select Configuration > Security.
3. In the navigation panel on the left, select Security Providers.
5. In the Modify Security Providers page:
a. In the Name box, enter a descriptive name of your choice for this security provider instance.

b. In the Security Provider Type drop down, select Claims to Email Security Provider for SharePoint Online.

c. In the User Identity drop-down list, select the user identity that you created to crawl your SharePoint Online.

d. In the Security Provider section:

   i. In the drop-down list, select the provider that recognizes your users by their email addresses or active directory accounts (see "Configuring an Email Security Provider" on page 65 or "Configuring an Active Directory Security Provider" on page 1141).

Notes:

- Blocked users (admin Office 365, active users, settings, sign-in status) are not expanded to email users.

- The list of following SharePoint well-known claims are expanded to email users:
  - c:0(.s|true) (everyone)
  - c:0-.f|rolemanager|spo-grid-all-users (everyone but external)
  - c:0!.s|forms%3amembership [all federated (sync) and native (cloud) users]
ii. When needed, click Add, Edit, or Manage security providers respectively to create, modify, or manage email or active directory security providers.

e. In the Windows Azure Active Directory Module for Windows PowerShell box, ensure that the MSOnline.psd1 file is available at the default location (C:\Windows\System32\WindowsPowerShell\v1.0\Modules\MSOnline\MSOnline.psd1) on your Coveo Master server following the installation of the Windows Azure AD Module installation (see "Installing the Windows Azure AD Module for Windows PowerShell" on page 1331). Change the path if needed.

Notes:

- Windows PowerShell is used to retrieve Office 365 users and domains.
- The default value should be the right value, but make sure the referenced module is installed and is located at this path.

f. Ensure that the Allow Complex Identities option is selected.

g. Click Save.

h. This security provider must be selected in the Security Provider for SharePoint Users parameter of the SharePoint security provider set on your SharePoint or OneDrive for Business source.

What's Next?

Create an Office 365 security provider that will use this Claims to Email security provider (see "Creating an Office 365 Security Provider for SharePoint Online" on page 1332).

9.31.6 Creating a Claims Security Provider for SharePoint Online

When indexing content from a SharePoint Online Web Application using Claims-based authentication, you must create a Claims security provider to allow authenticated users to search for documents secured using Claims permissions. Without such a security provider, no results would be returned.

The role of the Claims security provider is to authenticate users in SharePoint Online to retrieve the list of Claims associated to each user. Knowing the Claims of a user, the Coveo Search can display the search results this user is entitled to see according to the permissions that were indexed on SharePoint documents.

In order to be authenticated by the Claims security provider, a user must log in to the Coveo search interface using his SharePoint Online credentials. The Claims security provider can authenticate users in SharePoint Online using a native Office 365 identity or an identity provided by an ADFS server if Single Sign-On is enabled in SharePoint Online.
Notes:

- Coveo .NET Front-End version 12.0.99+ (March 2013 monthly release) is required to display search results with Claims permissions.
- The SharePoint, SharePoint Legacy and OneDrive for Business (CES 7.0.8047+ (December 2015)) connectors can use the Claims for SharePoint Online security provider type.
- You can get familiar with how Coveo components deal with permissions on documents both at indexing and query time.

To create a Claims security provider for SharePoint Online

1. On the Coveo server, access the Administration Tool.
2. In the Administration Tool, select Configuration > Security.
3. In the navigation panel on the left, select Security Providers.
5. In the Modify Security Providers page:
a. In the **Name** box, enter a descriptive name of your choice for this security provider instance.

b. In the **Security Provider Type** drop down, select **Claims for SharePoint Online**.

c. In the **User Identity** drop-down list:
   
   - When a claims-aware Coveo Search is used (see "Configuring the Claims-Aware Coveo Search Application" on page 183), select a user identity of any Windows account that can be used to authenticate to ADFS.
   
   - Otherwise, select the user identity that you created with an Office 365 account.

d. In the **SharePoint Web Application Url** box, enter the URL of the SharePoint Online Web Application where the secured content to index is located.

e. In the **Temporary path for the cache of User Claims** box, you must enter the path where the temporary cache of user Claims is saved.

f. In the **Office 365 Native Users Domain(s)** box, enter the domain name that was created with your Office
365 account. The domain name to enter here must be the native domain created by Microsoft Online Services, which is different from a private domain owned by your company (see "Finding Your Office 365 Native Domain Name" on page 111).

Note: You can enter more than one Office 365 domain, separating values by a comma.

g. Select the Single Sign-On (AD FS) is enabled check box when Active Directory synchronization is activated in Office 365 and synchronized user accounts are used to log in to SharePoint Online.

Important: When using ADFS Claims Authentication, you need to make sure your ADFS environment meets the requirement for the Claims security provider (see "ADFS Server Requirements for a Claims Security Provider" on page 1330).

CES 7.0.5556+ (June 2013) The following parameters are required only when the Single Sign-On (AD FS) is enabled check box is selected:

i. In the Url of the SharePoint AD FS Server box, enter the URL of the ADFS server which is trusted by SharePoint.

Example: https://adfs.mydomain.com

Note: CES 7.0.6684+ (May 2014) The SharePoint connector supports indexing SharePoint online configured with Okta.

In this case, in the Url of the SharePoint AD FS Server box, enter the full path to your SharePoint Online ActiveClientSignInUrl that should be in the form:

https://acme.okta.com/app/office365/abcdefgGWUMNWLYGXF/sso/wsfed/active

You can find your SharePoint Online ActiveClientSignInUrl in Okta, in the sign on instructions of the Microsoft Office 365 application:

i. With an administrator account, log in into Okta.

ii. In the top menu, click Admin.

iii. In the administration panel, select Applications > Applications.

iv. In the Applications page, click Microsoft Office 365.

v. In the Microsoft Office 365 page, select the Sign On tab.

vi. In the Sign On tab, under Sign On Methods section, click View Setup Instructions.

vii. The ActiveClientSignInUrl is the value next to ActiveLogOnUri.

Ensure that you also set this ActiveClientSignInUrl for the SharePoint Security provider and the SharePoint source.

ii. In the Trust Identifier for SharePoint box, enter the Relying Party Trust identifier for the SharePoint web application (see "Finding the Relying Party Trust Identifier for a SharePoint Web Application" on page 111).

h. CES 7.0.5556+ (June 2013) The following parameters are required only when multiple ADFS servers are
used to authenticate users in SharePoint:

i. In the **Url of the Identity Provider AD FS Server** box, enter the URL of the ADFS server which is used as an Identity Provider for the ADFS server trusted by SharePoint.

ii. In the **Trust Identifier for the SharePoint AD FS Server** box, enter the Relying Party Trust identifier for the SharePoint ADFS server (see "Finding the Relying Party Trust Identifier for a SharePoint ADFS server" on page 112).

i. When the **Single Sign-On (AD FS) is enabled** check box is selected and a claims-aware Coveo Search is used (see "Configuring the Claims-Aware Coveo Search Application" on page 183), in the **Bootstrap Token Signing Certificate (.cer)** box, enter the path on the Coveo Master server where you saved the certificate used by ADFS to sign requests from the claims-aware Coveo search. If the requests are not signed by ADFS, leave this parameter empty.

j. In the **Authentication Cookies Sliding Session Expiration Time (in days)** box, enter the time interval, in days, during which the Claims of a user authenticated by the Claims security provider remains valid. Values smaller than one day are accepted (ex.: 0.5).

k. Next to **Parameters**, when instructed to do so by Coveo Support, click **Add Parameter** to add an hidden parameter by entering the parameter **Name** and **Value**.

**Note:** **CES 7.0.6830+ (July 2014)** The parameter **ClaimsMaximumSize** is used to set the maximum allowed size for a single Claims identity. The default value is **12288** (12 KB). A message similar to the following one appears in the CES Console and logs typically when a user with claims exceeding this limit logged in or performed a query:

The security provider "Claims" has encountered an exception: class CSP::SecurityException: The user 'user_name here' contains too much claims and will be rejected.

When this condition occurs, the search results that are secured by Claims permissions are not returned for the query.

l. Ensure that the **Allow Complex Identities** option is selected.

A Claims security provider may need additional parameters when you create identities. You can specify these additional parameters only when the **Allow Complex Identities** option is selected.

m. Click **Save**.

**What's Next?**

Create an Office 365 security provider that will use this Claims security provider (see "Creating an Office 365 Security Provider for SharePoint Online" on page 1332).

**9.31.7 ADFS Server Requirements for a Claims Security Provider**

SharePoint can use ADFS as a trusted identity provider. Your ADFS environment must meet the following requirements to allow the Coveo Claims security provider to authenticate users in SharePoint.
For single ADFS server environments

- SharePoint ADFS server endpoint
  
  The following ADFS service endpoint must be enabled on your ADFS server (see "Finding and Enabling the ADFS Service Endpoint URL Path" on page 110):
  
  /adfs/services/trust/2005/usernamemixed

For multiple ADFS server environments

- SharePoint ADFS server endpoint
  
  The following ADFS service endpoint must be enabled on the ADFS server which is trusted by SharePoint (see "Finding and Enabling the ADFS Service Endpoint URL Path" on page 110):
  
  /adfs/services/trust/2005/issuedtokenmixedsymmetricbasic256

- Identity Provider ADFS server endpoint
  
  The following ADFS service endpoint must be enabled on the ADFS server which is trusted by SharePoint ADFS server (see "Finding and Enabling the ADFS Service Endpoint URL Path" on page 110):
  
  /adfs/services/trust/2005/usernamemixed

9.31.8 Installing the Windows Azure AD Module for Windows PowerShell

The Windows Azure Active Directory Module for Windows PowerShell cmdlets can be used to accomplish many Windows Azure AD tenant-based administrative tasks such as user management, domain management and for configuring single sign-on (see Manage Azure AD using Windows PowerShell).

The Coveo Office 365 security provider needed by the SharePoint connector when indexing SharePoint Online content uses the Get-MsolGroupMember cmdlet to list users and groups that are members of a specific Office 365 security group (see Get-MsolGroupMember). In this case, you must install the Windows Azure Active Directory Module on your Coveo Master server.

To install the Windows Azure AD Module for Windows PowerShell

1. Using an administrator account, connect to the Coveo Master server.

2. Referring to the Microsoft documentation:
   
   a. Ensure that your Coveo Master server meets the following Windows Azure AD Module for Windows PowerShell requirements:
      
      - Microsoft .NET Framework 3.51 feature.
   
   b. Download and install the appropriate Microsoft Online Services Sign-In Assistant version for your operating system (see Microsoft Online Services Sign-In Assistant for IT Professionals RTW).

3. Install the Windows Azure Active Directory Module for Windows PowerShell (see Install the Windows Azure AD Module).
4. Connect to Windows Azure AD by running the PowerShell command `import-module MSOnline` (see Connect to Windows Azure AD).

What's Next?

When you configure the Office 365 security provider, ensure that the `C:\Windows\System32\WindowsPowerShell\v1.0\Modules\MSOnline\MSOnline.psd1` file is available on the Coveo Master server and referenced in the `Windows Azure Active Directory Module for Windows PowerShell` parameter (see Creating an Office 365 Security Provider for SharePoint Online).

9.31.9 Creating an Office 365 Security Provider for SharePoint Online

Because Office 365 security groups can be used as domain groups in SharePoint Online to set documents permissions, you must create an Office 365 security provider to allow authenticated users to search for documents secured using SharePoint Online domain groups.

The role of the Office 365 security provider is to resolve Office 365 security groups into its list of members.

Notes:

- **Coveo .NET Front-End 12.0.99+ (March 2013)** Support to display search results with Claims permissions.
- The SharePoint, SharePoint Legacy, and OneDrive for Business (CES 7.0.8047+ (December 2015)) connectors can use the Claims for SharePoint On-premises security provider type.
- You can get familiar with how Coveo components deal with permissions on documents both at indexing and query time.

To create an Office 365 security provider for SharePoint Online

1. On the Coveo server, access the Administration Tool.
2. In the Administration Tool, select **Configuration > Security**.
3. In the navigation panel on the left, select **Security Providers**.
4. In the **Security Providers** page, click **Add**.
5. In the **Modify Security Providers** page:
a. In the **Name** box, enter a descriptive name of your choice.

b. In the **Security Provider Type** drop down, select **Office 365**.

c. In the **User Identity** drop-down list, select the user identity that you created to crawl your SharePoint Online.

d. In the **Users Security Provider** drop-down list, select the Claims Security Provider for SharePoint Online or the Claims to Email Security Provider for SharePoint Online that you previously created ([CES 7.0.7433+ (February 2015)](https://www.coveo.com)) (see "Creating a Claims Security Provider for SharePoint Online" on page 1326 and Creating a Claims to Email Security Provider for SharePoint Online).

e. In the **Windows Azure Active Directory Module for Windows PowerShell** box, ensure that the MSOnline.psd1 file is available at the default location (C:\Windows\System32\WindowsPowerShell\v1.0\Modules\MSOnline\MSOnline.psd1) on your Coveo Master server following the installation of the Windows Azure AD Module installation (see "Installing the Windows Azure AD Module for Windows PowerShell" on page 1331). Change the path if needed.

   **Note:** You need to install the Windows Azure AD Module version with the same word size (32-bit vs 64-bit) as your version of CES. If you install the 64-bit version of the Windows Azure AD Module and run the 32-bit version of CES, when the connector requires the module, Windows will silently attempt to load the 32-bit version of the AD module, even if you specified the path for the 64-bit version.

f. Leave the **Allow Complex Identities** option cleared as it does not apply to this type of security provider.

g. Click **Save**.
What's Next?
Create a SharePoint security provider that will use this Claims security provider.

9.32 Microsoft SharePoint Legacy Connector

**Deprecated**
The Coveo Legacy connector for Microsoft SharePoint allows you to bring the information stored on one or multiple SharePoint farms into the unified index so that end-users can easily access this content. The Legacy connector allows Coveo Enterprise Search (CES) to crawl and index a complete SharePoint farm or specific farm sections, such as Web Applications, site collections, websites, lists, or document libraries.

**Note:** A second generation SharePoint connector is now available and strongly recommended to use over the legacy version.

**CES 7.0.7433+ (February 2015)** A tool to convert your SharePoint Legacy sources to SharePoint sources is available. The SharePoint Converter Tool, which is compatible with CES 7.0.6767+ (June 2014 monthly release), is pretty useful when you want to take full advantage of the improved SharePoint connector without having to recreate all your SharePoint Legacy sources. Contact Coveo Support to get the SharePoint Converter Tool.

9.32.1 Connector Features Summary

<table>
<thead>
<tr>
<th>Features</th>
<th>Supported</th>
<th>Additional information</th>
</tr>
</thead>
<tbody>
<tr>
<td>SharePoint version</td>
<td>2010, 2013, Online, Foundation 2010, and Foundation 2013</td>
<td>Farms (tenant in SharePoint Online), Web applications, site collections, sites, subsites, portals(^1), areas, area listings, user profiles(^1), personal websites(^1), lists(^1), list items(^<em>), list item attachments(^</em>), document libraries, document sets, documents, Web parts(^2), and microblog posts and replies. Note: Unpublished items are indexed.</td>
</tr>
<tr>
<td>Searchable content types</td>
<td>✔️</td>
<td></td>
</tr>
<tr>
<td>Content update</td>
<td>Incremental refresh ✔️</td>
<td>Full refresh or rebuild is needed to retrieve updated (added, created, deleted) user profiles(^1).</td>
</tr>
<tr>
<td></td>
<td>Full refresh ✔️</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Rebuild ✔️</td>
<td></td>
</tr>
<tr>
<td>Document-level security</td>
<td>✔️</td>
<td></td>
</tr>
</tbody>
</table>

\* - Not supported for SharePoint Online.
1 - Not available in Microsoft SharePoint Foundation.

2 - Not all Web parts are available in Microsoft SharePoint Foundation 2010 (see Overview of Web Parts available in SharePoint Foundation 2010).

9.32.2 Features

- Content indexing
  - Indexing all SharePoint content
    - Farms and Web Applications
    - Site collections and sites
    - Portals, areas, and area listings
      
        **Note:** Portals are not available in Microsoft SharePoint Foundation.

    - Lists, list items, and list item attachments
      
        **Note:** Not supported for SharePoint Online.

    - Document libraries, documents, and document sets
    
      - User profiles and personal websites
        
          **Note:** User profiles and personal websites are not available in Microsoft SharePoint Foundation.

  - Web Parts

    **Note:** Not all Web parts are available in Microsoft SharePoint Foundation 2010 (see Overview of Web Parts available in SharePoint Foundation 2010).

    - CES 7.0.5556+ (June 2013) Microblog posts and replies

      - Automatic site collection discovery

        You can configure the SharePoint Legacy connector to index all site collections located on a SharePoint farm without having to list them manually (see SharePoint Site Discovery in Configuring and Indexing a Microsoft SharePoint Source).

      - HTTP over SSL (HTTPS) support

        You can use the SharePoint Legacy connector to index a SharePoint site that uses HTTPS.

- Security

  The SharePoint Legacy connector supports security for SharePoint Web Applications using Classic Mode or Claims Based authentication.
Classic Mode

The Legacy connector indexes permissions on SharePoint items as SharePoint groups and Windows accounts.

- When a user performs a query, returned results are only those to which his Windows account has access.
- Users can perform queries from any CES search interface.

- **CES 7.0.5031+ (March 2013)** Claims Based (Forms, Windows [NTLM or Kerberos], ADFS)

  The Legacy connector indexes permissions on SharePoint items as SharePoint groups and Claims.

  - When a user performs a query, returned results are only those with permissions that match any of the Claims assigned to the user after he is successfully authenticated in SharePoint.

  - Users can perform queries from any Coveo search interface:
    - When searching from within SharePoint using the Coveo search box, the user is already authenticated in SharePoint and his Claims are available to the Coveo Search. This means that search queries can be performed using the Claims assigned to the user.
    - Claims users can also perform searches for secured SharePoint content from Coveo search interfaces outside SharePoint without having to log in to the search interface (see "Manually Configuring a .NET Search Interface Claims SSO for an On-Premises SharePoint" on page 178).

Note: When configuring a SharePoint Legacy connector source, you must select an **Authentication Type** (see "Configuring and Indexing a Microsoft SharePoint Source With the Legacy Connector" on page 1345). The selection depends on the type of authentication used by the SharePoint Web Application Zone that the source indexes.

The SharePoint Legacy connector supports indexing content from SharePoint Web Applications using the following Claims authentication types:

- Windows authentication
- Form-based authentication
- **CES 7.0.5556+ (June 2013)** Trusted identity provider (ADFS)

- Incremental refresh

  Once incremental refresh is enabled on a SharePoint source, the SharePoint Legacy connector automatically refreshes the content modified since the last incremental refresh run. This way, the index is always kept up to date.

- SharePoint Integration:
  - Installation of Coveo Web Service on the SharePoint server to provide more crawling functions
  - Installation of the Coveo search box to replace the SharePoint search box
  - Installation of Coveo search interfaces on the SharePoint server

- **Intranet** and **SharePoint** search interface features related to the SharePoint Legacy connector:
Search results folding for the following SharePoint items:

- Blog posts and their comments
- Discussion board threads
- Document sets and their items

The Document Sets facet appears, listing all document sets included in the results when one or more document set items match the query.

Search results referring to a document link in SharePoint are now identified with a special icon.

### Feature history

<table>
<thead>
<tr>
<th>CES version</th>
<th>Monthly release</th>
<th>Features</th>
</tr>
</thead>
<tbody>
<tr>
<td>7.0.6830</td>
<td>July 2014</td>
<td>Source and security provider types renamed from SharePoint to SharePoint Legacy with the introduction of the second generation SharePoint connector.</td>
</tr>
<tr>
<td>7.0.6424</td>
<td>February 2014</td>
<td>Search interface with Claims SSO (see &quot;Manually Configuring a .NET Search Interface Claims SSO for an On-Premises SharePoint&quot; on page 178)</td>
</tr>
</tbody>
</table>
| 7.0.5556    | June 2013       | • Beta support for SharePoint 2013 Online.  
• Support Conversations (Micro-Blogging)  
• Trusted identity provider (ADFS) |
| 7.0.5031    | March 2013      | Beta support for an on-premises SharePoint 2013 and SharePoint 2010 Online. Claims-based authentication for any search interface. |
| 7.0.4855    | August 2012     | Support for Claims-based authentication for search interfaces integrated in SharePoint |

### 9.32.3 Microsoft SharePoint Legacy Connector Deployment Overview

** Deprecated **

The following procedure outlines the steps needed to deploy the Microsoft SharePoint Legacy connector. The steps indicate the order in which you must perform configuration tasks in Microsoft SharePoint and CES.

**Note:** It is strongly recommended to rather use the second generation SharePoint connector.

1. Validate that your environment meets the requirements (see "Microsoft SharePoint Legacy Connector Requirements" on page 1338).

2. Identify if the SharePoint environment you want to index is a **Classic**, **Claims**, or **Online** type (see "Identifying Your SharePoint Environment" on page 1339).

3. On your SharePoint farm (tenant in SharePoint Online):
a. Select or create a user that the Legacy connector will use to crawl your SharePoint content. The type of user depends on the type of SharePoint environment (see "Type of User to Specify for the User Identity" on page 1340).

b. Grant appropriate SharePoint permissions to the crawling account you selected (see "Granting SharePoint Permissions to the Crawling Account" on page 1307).

c. For on-premises environments, install the Coveo web service, search box, and search interface on your SharePoint farm (see "Installing the Coveo Web Service, Search Box, and Search Interface into SharePoint" on page 1309).

Note: With this installation procedure, you can also integrate the Coveo search box to SharePoint. This is not needed to deploy the Legacy connector and can be done later.

4. On the Coveo Master server, in the Administration Tool:

a. Configure the user identity

Once the crawling account has been set up, you must create a CES user identity for this account.

b. When indexing SharePoint Online content, you must install the Windows Azure AD module on the Coveo Master server because it is needed by the Office 365 security provider (see "Installing the Windows Azure AD Module for Windows PowerShell" on page 1331).

c. Determine which security providers are required for your SharePoint environment (see "Security Providers to Use" on page 1340).

Create the required ones:

- "Creating a Claims Security Provider for an On-Premises SharePoint" on page 1319
- "Creating a Claims Security Provider for SharePoint Online" on page 1326
- "Creating an Office 365 Security Provider for SharePoint Online" on page 1332
- "Creating a Security Provider for the SharePoint Legacy Connector" on page 1341

d. Configure and index the Microsoft SharePoint source

The Coveo Legacy connector needs to know details about your Microsoft SharePoint server or farm (tenant in SharePoint Online) to be able to index its content (see "Configuring and Indexing a Microsoft SharePoint Source With the Legacy Connector" on page 1345).

5. When you provide a Coveo .NET search interface residing outside SharePoint and want users to be able to find Claims-secured SharePoint content without having to log in again to SharePoint, configure the search interface to manage single sign-on (see "Manually Configuring a .NET Search Interface Claims SSO for an On-Premises SharePoint" on page 178).

9.32.4 Microsoft SharePoint Legacy Connector Requirements

Deprecated

Your environment must meet the following requirements to be able to use the Coveo Legacy connector for Microsoft SharePoint.
9.32.4.1 Requirements

- Coveo license for the Microsoft SharePoint Legacy connector
  
  Your Coveo license must include support for the Microsoft SharePoint Legacy connector to be able to use this connector.

- Appropriate SharePoint permissions for the crawling account (see "Granting SharePoint Permissions to the Crawling Account" on page 1307).

**Note:** For environment using Claims, also refer to the Claims security provider requirements (see "ADFS Server Requirements for a Claims Security Provider" on page 1330).

9.32.4.2 SharePoint Supported Versions

- SharePoint Online

- SharePoint 2013
  
  - CES 7.0.5031+ (March 2013) On-premises (Beta)
  
- Microsoft SharePoint Foundation 2013

- SharePoint 2010
  
  - Microsoft SharePoint Foundation 2010 (WSS 4)
  
- Microsoft SharePoint 2010 (SharePoint 2010)

- SharePoint 2007
  
  - Windows SharePoint Services 3.0 (WSS 3)
  
- Microsoft Office SharePoint Server 2007 (MOSS 2007)

**Note:** The Coveo Platform 7 does not support the legacy SharePoint 2003.

What's Next?

Select or create a user that the Legacy connector will use to crawl your SharePoint content, and then grant appropriate SharePoint permissions to this crawling account (see "Granting SharePoint Permissions to the Crawling Account" on page 1307).

9.32.5 Identifying Your SharePoint Environment

**Deprecated**

The SharePoint Legacy connector supports on-premises and online SharePoint versions (see "Microsoft SharePoint Legacy Connector Requirements" on page 1338). The connector components to deploy vary depending on the SharePoint environment being indexed.

Before starting to deploy the Legacy connector, you must refer to the following table and identify the SharePoint environment type from which you want to index content (Classic, Claims, or Online).
9.32.5.1 Security Providers to Use

Your SharePoint environment to index determines the required security providers that you must create.

<table>
<thead>
<tr>
<th>Required security provider type</th>
<th>SharePoint environment</th>
</tr>
</thead>
<tbody>
<tr>
<td>SharePoint</td>
<td>Classic</td>
</tr>
<tr>
<td>Active Directory</td>
<td>✓</td>
</tr>
<tr>
<td>Claims for SharePoint On-premises</td>
<td></td>
</tr>
<tr>
<td>Claims for SharePoint Online</td>
<td></td>
</tr>
<tr>
<td>Office 365</td>
<td></td>
</tr>
</tbody>
</table>

**Note:** When you want to index content from different SharePoint environments, you must create multiple SharePoint security provider and source instances, each one with its own configuration.

9.32.5.2 Type of User to Specify for the User Identity

Your SharePoint environment to index determines the type of user that you must specify in a User Identity to allow the Legacy connector and security provider to crawl your SharePoint content.

<table>
<thead>
<tr>
<th>SharePoint environment</th>
<th>Enabled authentication</th>
<th>Type of user</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>Classic</td>
<td>Windows</td>
<td>Windows account</td>
<td>acme\john</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td><a href="mailto:john@acme.com">john@acme.com</a></td>
</tr>
<tr>
<td>Claims</td>
<td>Windows</td>
<td>Windows account</td>
<td>acme\john</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td><a href="mailto:john@acme.com">john@acme.com</a></td>
</tr>
<tr>
<td></td>
<td>Form</td>
<td>Format expected by the login form</td>
<td></td>
</tr>
<tr>
<td>SharePoint environment</td>
<td>Enabled authentication</td>
<td>Type of user</td>
<td>Example</td>
</tr>
<tr>
<td>------------------------</td>
<td>------------------------</td>
<td>-----------------------------------</td>
<td>--------------------------</td>
</tr>
<tr>
<td>ADFS</td>
<td>Federated by ADFS</td>
<td>acme\john</td>
<td><a href="mailto:john@acme.com">john@acme.com</a></td>
</tr>
<tr>
<td>Online</td>
<td>Native</td>
<td>Native Office 365 account</td>
<td><a href="mailto:john@acme.onmicrosoft.com">john@acme.onmicrosoft.com</a></td>
</tr>
<tr>
<td>SSO</td>
<td>Single Sign-On Office 365 account</td>
<td><a href="mailto:john@acme.com">john@acme.com</a></td>
<td></td>
</tr>
</tbody>
</table>

**Note:** You will create a User Identity with the credentials of the selected user. You will then assign the User Identity to one or more security providers and to the source.

**What's Next?**

Grant appropriate SharePoint permissions to the selected crawling account (see "Granting SharePoint Permissions to the Crawling Account" on page 1307).

### 9.32.6 Creating a Security Provider for the SharePoint Legacy Connector

**Deprecated**

A SharePoint source created with the SharePoint Legacy connector needs a SharePoint security provider to resolve permissions found on documents in the unified indexed. These permissions can either be SharePoint groups, users, or domain groups. Of these three types of permissions, only SharePoint groups are actually processed by the SharePoint security provider. Users and domain groups are simply forwarded to other security providers for processing.

The other types of security providers required to process users and domain groups vary according to the SharePoint environment being indexed, more precisely, according to the type of authentication provider (Classic Windows, Claims-Based) used by the Web Application, and the SharePoint server version (2013/2010/2007 on-premises and Online).

For this reason, before going on with the configuration of the SharePoint security provider, if not already done, you must identify the type of your SharePoint environment from which you will be indexing content (see "Identifying Your SharePoint Environment" on page 1339).

**Notes:**

- **CES 7.0.6830+ (July 2014)** It is recommended to rather use the second generation SharePoint connector to create your source. If you do so, ensure to use the corresponding SharePoint security provider type.

- You can get familiar with how Coveo components deal with permissions on documents both at indexing and query time.

To modify or configure a SharePoint security provider

1. On the Coveo server, access the Administration Tool.
2. Select **Configuration > Security**.
3. In the **Security** page, in the navigation panel on the left, click **Security Providers**.

4. In the **Security Providers** page, click **Add**.

5. In the **Modify Security Provider** page:
a. In the **Name** box, enter a name to identify this security provider.

   **Example:** SharePoint Security Provider (Classic)

b. In the **Security Provider Type** drop-down list, select **SharePoint Legacy (x64)** (or **SharePoint (x86)** on a 32-bit Coveo server).

   **Notes:**
   - **CES 7.0.6830+ (July 2014)** The **SharePoint (x64)** type corresponds to the security provider to be used with the second generation SharePoint connector.
   - **CES 7.0.6767– (June 2014)** The **SharePoint Legacy (x64)** security provider type was named **SharePoint (x64)**.

c. In the **User Identity** section:
   - i. In the drop-down list, select the user identity that you selected or created previously for this connector (see "Type of User to Specify for the User Identity" on page 1340).
   - ii. When needed, click **Add, Edit, or Manage user identities** respectively to create, modify, or manage user identities.

   **Note:** The User Identity specified here will be relevant later on in this topic when selecting the value of the **Authentication Type** parameter.

d. In the **Temporary path** box, enter the path for the temporary security provider working folder on the Coveo server. If not specified, a temporary working folder will be created by the security provider.

   **Example:** C:\temp

e. In the **SharePoint Server Url** box, enter the following value according to your SharePoint environment:

   - **Classic** and **Online**: leave blank.
   - **Claims**: URL of the SharePoint Web Application where the Coveo SharePoint Web Service is installed (see "Installing the Coveo Web Service, Search Box, and Search Interface into SharePoint" on page 1309).

f. In the **Active Directory Security Provider** drop-down list, for all SharePoint environments, select the Active Directory security provider.

g. **CES 7.0.5031+ (March 2013)** In the **Security Provider for SharePoint Users** drop-down list, select the following Security Provider according to your SharePoint environment.

   - **Classic**: Select the **Active Directory** security provider.
   - **Claims**: Select your Claims security provider for an on-premises SharePoint (see "Creating a Claims Security Provider for an On-Premises SharePoint" on page 1319).
   - **Online**: 

[www.coveo.com](http://www.coveo.com)
Select your Claims security provider for SharePoint Online (see "Creating a Claims Security Provider for SharePoint Online" on page 1326).

OR

Select your Claims to Email security provider for SharePoint Online (see "Creating a Claims to Email Security Provider for SharePoint Online" on page 1324).

In the Security Provider for Domain Groups drop-down list, select the following Security Provider according to your SharePoint environment.

- **Classic**: Select the Active Directory security provider.
- **Claims**: Select your Claims security provider for an on-premises SharePoint (see "Creating a Claims Security Provider for an On-Premises SharePoint" on page 1319).
- **Online**: Select your Office 365 security provider (see "Creating an Office 365 Security Provider for SharePoint Online" on page 1332).

In the Connection timeout box, consider changing the time interval the connector waits to establish the connection with the SharePoint server. The default value is 30000 mS.

In the Timeout retry box, consider changing the number of times the connector retries to connect with the SharePoint server before throwing an error. The default value is 3 retries.

In the Get changes timeout box, consider changing the time interval the connector waits to get changes from the SharePoint server. The default value is 15000 mS.

In the Authentication Type box, enter one of the following types of authentication according to your SharePoint environment:

- **Classic**: Enter Default.
- **Claims**: If the User Identity specified on this security provider was:
  - A Windows account, enter: WindowsUnderClaims
  - Form authentication credentials, enter: FormsUnderClaims
  - ADFS federated account, enter: AdfsUnderClaims
- **Online**: If the User Identity specified on this security provider was:
  - A native Office 365 user account (ex.: john@acme.onmicrosoft.com), enter: OnlineUnderClaims
  - A single sign-on Office 365 account (ex.: john@acme.com), enter: OnlineFederated

**Note**: The Authentication Type specified here is determined by the User Identity parameter that was specified earlier in this topic.

The following ADFS related parameters are only required when the Authentication Type is either AdfsUnderClaims or OnlineFederated.
i. In the **Url of the SharePoint AD FS Server** box, enter the URL of the ADFS server which is trusted by SharePoint.

ii. In the **Trust Identifier for SharePoint** box, enter the Relying Party Trust identifier for the SharePoint web application (see "Finding the Relying Party Trust Identifier for a SharePoint Web Application" on page 111).

The following parameters are required only when multiple ADFS servers are used to authenticate users in SharePoint:

i. In the **Url of the Identity Provider AD FS Server** box, enter the URL of the ADFS server which is used as an Identity Provider for the ADFS server trusted by SharePoint.

ii. In the **Trust Identifier for the SharePoint AD FS Server** box, enter the Relying Party Trust identifier for the SharePoint ADFS server (see "Finding the Relying Party Trust Identifier for a SharePoint AD FS server" on page 112).

**Note:** At this point, the proper ADFS endpoint(s) should already have been enabled on the ADFS server(s) during the configuration of the Claims for SharePoint 2010 Online security provider (see "ADFS Server Requirements for a Claims Security Provider" on page 1330).

n. Leave the **Allow Complex Identities** option cleared as it does not apply to this type of security provider.

o. In the **Parameters** section, in rare cases the Coveo Support could instruct you to click **Add Parameters** to specify other security provider parameter names and values that could help to troubleshoot security provider issues.

6. Click **Apply Changes**.

What's Next?

Configure and index a Microsoft SharePoint source (see "Configuring and Indexing a Microsoft SharePoint Source With the Legacy Connector" on page 1345).

9.32.7 Configuring and Indexing a Microsoft SharePoint Source With the Legacy Connector

**Deprecated**

A source defines a set of configuration parameters to extract and index Microsoft SharePoint content. This topic describes how to create a source using the SharePoint Legacy connector.

**Notes:**

- In an environment with more than one Microsoft SharePoint Web Application, it is recommended to define one source for each Microsoft SharePoint Web Application that you want to index, and only index user profiles once to not create duplicates in your index.

- **CES 7.0.6830+ (July 2014)** The original **SharePoint** connector was renamed to **SharePoint Legacy**. The **SharePoint** source type now corresponds to the second generation SharePoint connector that is recommended to use.
To configure and index a Microsoft SharePoint source

1. On the Coveo server, access the Administration Tool.

2. Select **Index > Sources and Collections**.

3. In the **Collections** section:
   
   a. Select an existing collection in which you want to add the new source.

   OR

   b. Click **Add** to create a new collection.

4. In the **Sources** section, click **Add**.

   The **Add Source** page that appears is organized in three sections.

5. In the **General Settings** section of the **Add Source** page:

   a. Enter the appropriate value for the following required parameters:

   **Name**

   Enter a descriptive name of your choice for the source.

   **Example**: SharePoint Intranet
Source Type

**CES 7.0.7814+ (August 2015)** The connector used by this source. In this case, select SharePoint (deprecated).

Notes:

- If you do not see SharePoint (deprecated) in the Source Type list, your environment does not meet the requirements (see "Microsoft SharePoint Legacy Connector Requirements" on page 1338).

**CES 7.0.7711– (June 2015)** The SharePoint (deprecated) source type is named SharePoint Legacy.

**CES 7.0.6767– (June 2014)** The SharePoint Legacy source type is named SharePoint.

**CES 7.0.6830+ (July 2014)** The SharePoint type corresponds to the source to be used with the second generation SharePoint connector.

Addresses

List of specific SharePoint farm sections that you want to index. If you need to index more than one section, enter one URL per line.

Examples:

- For the whole farm:
  
  https://farm/

- For a specific Web Application:

  https://farm:8080/

- For a specific site collection:

  https://farm:8080/sites/Support/default.aspx

- For a specific website:


- For a specific document library:

  https://farm:8080/Document Library/

- For a specific list:

  https://farm:8080/sites/Support/Lists/Contacts/AllItems.aspx

  **Important:** A specific folder in a list is not supported.

- For SharePoint Online:

  https://domain.sharepoint.com
Refresh Schedule

Time interval at which the index is automatically refreshed to keep the index content up-to-date. The incremental refresh continuously takes care of indexing ongoing SharePoint content changes. You can select to refresh the source weekly by selecting the Every Sunday option.

**Note:** You can create new or modify existing source refresh schedules.

b. Review the value for the following parameters that often do not need to be modified:

**Rating**

Change this value only when you want to globally change the rating associated with all items in this source relative to the rating to other sources.

**Example:** If this source was for a legacy Intranet, you may want to set this parameter to Low, so that in the search interface, results from this source appear later in the list compared to those from other sources.

**Document Types**

If you defined custom document type sets, ensure to select the most appropriate for this source.

**Active Languages**

If you defined custom active language sets, ensure to select the most appropriate for this source.

**Fields**

If you defined custom field sets, ensure to select the most appropriate for this source.

6. In the **Specific Connector Parameters & Options** section of the Add Source page, review if you need to change the parameter default values:

   a. In the **SharePoint References** drop-down list, select the appropriate SharePoint reference set for this source.

      **Note:** You can define custom SharePoint references.
b. In the Option section:

**Index personal sites**

*Note:* Personal websites are not available in Microsoft SharePoint Foundation.

When selected, indexes all the personal sites of the SharePoint farm (tenant in SharePoint Online). This option is selected by default.

**Index user profiles**

When selected, indexes all the user profiles of the SharePoint farm (tenant in SharePoint Online). This option is selected by default.

**Notes:**

- Indexing user profiles can take a significant time depending on their number. Moreover, indexing user profiles more than once, creates as many duplicates in your index. It is thus recommended to only index your user profiles once for all your SharePoint sources:
  - When you configure your first SharePoint source, let the check box selected. For all you other SharePoint sources, clear the check box.
  - When you already have other configured SharePoint source(s), look for your smallest Web Application in size and clear the **Index user profiles** check box for all your other SharePoint sources.
- User profiles are not available in Microsoft SharePoint Foundation.

**Index subsites**

When selected, indexes subsites recursively, starting with the URLs entered in the **Addresses** box, and proceeding to deeper levels until every document has been indexed. This option is selected by default.

**Example:** When `http://intranet/pages/` is a URL entered in the **Addresses** box and **Index subsites** is selected, the `http://intranet/pages/news/` and `http://intranet/pages/news/2012/` websites are also indexed.

**Index the document’s metadata**

When selected, CES indexes all the document metadata, even metadata that are not associated with a field. The orphan metadata are added to the body of the document so that they can be searched using free text queries.

When cleared (default), only the values of system and custom fields that have the **Free Text Queries** attribute selected will be searchable without using a field query.
Example: A document has two metadata:
- LastEditedBy containing the value Hector Smith
- Department containing the value RH

In CES, the custom field CorpDepartment is bound to the metadata Department and its Free Text Queries attribute is selected.

When the Index the document's metadata option is cleared, searching for RH returns the document because a field is indexing this value. Searching for hector does not return the document because no field is indexing this value.

When the Index the document's metadata option is selected, searching for hector also returns the document because CES indexed orphan metadata.

Generate a cached HTML version of indexed documents

When you select this check box (recommended), at indexing time, CES creates HTML versions of indexed documents. In the search interfaces, users can then more rapidly review the content by clicking the Quick View link rather than opening the original document with the original application. Consider clearing this check box only if you do not want to use Quick View links.

Open results with cached version

Leave this check box cleared (recommended) so that in the search interfaces, the main search result link opens the original document with the original application. Consider selecting this check box only when you do not want users to be able to open the original document but only see the HTML version of the document as a Quick View. In this case, you must also select Generate a cached HTML version of indexed documents.

c. In the SharePoint Site Discovery section, specify which SharePoint site collections to index by selecting one of the following options:

Index only starting addresses

Indexes only the sites (and subsites when the Index subsites option is selected) whose addresses are entered in the Addresses box.

Index the starting addresses and all sites listed in the Portal Site Directory

Indexes the sites (and subsites when the Index subsites option is selected) whose URLs are entered in the Addresses box as well as all sites, related to these addresses, listed in the portal site directories.

Index the Web application of the starting addresses

Indexes all site collections of the Web Applications related to the starting addresses. The default choice.

Index all the Web applications having the same host name

Indexes all site collections of all Web Applications related to the starting addresses, as long as the Web Application has the same host as its related starting address.
7. In the Security section of the Add Source page:

   a. In the SharePoint Security Provider drop-down list, you must select a security provider of type SharePoint (see "Creating a Security Provider for the SharePoint Legacy Connector" on page 1341).

   b. In the Authentication drop-down list, select the user identity that you created for the Microsoft SharePoint farm (tenant in SharePoint Online).

   c. CES 7.0.5031+ (March 2013) In the Authentication Type section, select the type of authentication used to access the SharePoint web services:

      Windows (Classic)
      Select for Web Applications that use classic authentication (NTLM or Kerberos), not Claims.

      Forms (Claims)
      Select for Claims-enabled Web Applications that use form authentication.

      Windows (Claims)
      Select for Claims-enabled Web Applications that use Windows authentication (NTLM or Kerberos).
AD FS (Claims) CES 7.0.5556+ (June 2013)

Select for Claims-enabled Web Applications that use ADFS as a trusted identity provider.

Office 365 (Native)

Select when crawling a SharePoint Online Web Application using a native Office 365 user account (ex: john@acme.onmicrosoft.com).

Office 365 (Single sign-on)

Select when crawling a SharePoint Online Web Application using a single sign-on Office 365 user account (ex: john@acme.com).

d. CES 7.0.5556+ (June 2013) The following ADFS related parameters are only required when the Authentication Type is either AD FS (Claims) or Office 365 (Single sign-on):

i. In the Url of the SharePoint AD FS Server box, enter the URL of the ADFS server which is trusted by SharePoint.

ii. In the Trust Identifier for SharePoint box, enter the Relying Party Trust identifier for the SharePoint web application (see "Finding the Relying Party Trust Identifier for a SharePoint Web Application" on page 111).

The following parameters are required only when multiple ADFS servers are used to authenticate users in SharePoint

i. In the Url of the Identity Provider AD FS Server box, enter the URL of the ADFS server which is used as an Identity Provider for the ADFS server trusted by SharePoint.

ii. In the Trust Identifier for the SharePoint AD FS Server box, enter the Relying Party Trust identifier for the SharePoint ADFS server (see "Finding the Relying Party Trust Identifier for a SharePoint ADFS server" on page 112).

e. Click Save to save the source configuration and consider revising advanced source parameters before starting indexing the new source (see "Modifying Hidden Microsoft SharePoint Source Parameters for the Legacy Connector" on page 1353).

OR

f. Click Save and Start to save and start indexing immediately.

Note: When your SharePoint Web Application uses Claims, the first time the SharePoint search interface is accessed, the first time setup page appears with two panels to let you enter your Claims information and allow access to the search interface (see "Coveo .NET Front-End First Time Setup" on page 47).

What's Next?

Set an incremental refresh schedule for your source.

Consider modifying advanced source parameters (see "Modifying Hidden Microsoft SharePoint Source Parameters for the Legacy Connector" on page 1353).
9.32.7.1 Modifying Hidden Microsoft SharePoint Source Parameters for the Legacy Connector

**Deprecated**

After you created a SharePoint source, you can modify a number of advanced parameters to fine-tune indexing of your SharePoint content.

**Note:** You need to rebuild your source after changing advanced parameters.

To modify SharePoint advanced source parameters

1. On the Coveo server, access the Administration Tool.
2. Select **Index > Sources and Collections**.
3. In the **Collections** section, select the collection containing the SharePoint source for which you want to change advanced parameters.
4. In the **Sources** section, select the SharePoint source.
5. In the navigation panel on the left, select **Advanced**.
6. In the **Advanced** page:
a. In the **Crawling** section, select the desired crawling options:

**Index hidden lists and their items**

Specifies whether hidden lists should be indexed or not. SharePoint uses hidden (or internal) lists to store non content information, such as Web Part galleries, work flow state, etc. These lists and their list items are not indexed by default.

**Index redundant issue list items**

Specifies whether redundant issues should be indexed or not. When an issue is updated in a SharePoint issue list, SharePoint creates a new issue item, leaving the old one unchanged. These redundant old issues are not indexed by default.

**Index survey responses**

Specifies whether survey responses should be indexed or not. When someone responds to a SharePoint survey, this response is stored as a list item into the survey list. These responses are not indexed by default.
Index documents uploaded with WebDAV

Specifies whether orphan documents should be indexed or not. Using the WebDAV functionality, it is possible to store documents that do not belong to any SharePoint document libraries. These documents are indexed by default.

Index social tags

Specifies whether social tags should be indexed or not. In SharePoint 2010, users can tag content to categorize information in ways that are meaningful to them. Social tagging can improve the quality of search results by filtering against specific tags. The social tags are not indexed by default. When selected, this option slightly affects crawling performances.

**Note:** Only public social tags are indexed, not personal social tags.

Disable cookies

Specifies whether the connector should cache and reuse the cookies sent by the crawled site. The cookies are enabled by default.

Expand sites and lists before applying filters

Specifies whether the connector should retrieve the SharePoint websites and list children before applying the source filters. This option is required to index a specific part of a SharePoint website or list. This option is disabled by default.

**Note:** Enabling this option slows down the connector as it retrieves all children of all websites and lists from SharePoint and rejects filtered documents just before indexing them.

**Example:** When [http://intranet/](http://intranet/) is the main website, [http://intranet/pages/*](http://intranet/pages/*) is the only source inclusion filter, and **Expand sites and lists before applying filters** is selected, [http://intranet/pages/](http://intranet/pages/) and [http://intranet/pages/news/](http://intranet/pages/news/) websites are indexed. When **Expand sites and lists before applying filters** is not selected, nothing will be indexed as [http://intranet/](http://intranet/) will be filtered out.

Use the author extracted from the document instead of the SharePoint author

A document stored in a SharePoint document library may have two different authors, the author of the document stored in the document properties and the author stored in the SharePoint database, which represents the person who has modified or added the document into SharePoint. By default, CES uses the SharePoint author instead of the document author. Select this option to modify this behavior.

**Note:** A side effect of selecting this option is that the CES SharePoint search interface cannot link the search result author to the SharePoint user, as the document author may not be a SharePoint user.

Enable Microsoft Office integration

Specifies whether Microsoft Office documents should be opened directly within SharePoint (using SharePoint ActiveX) when the user clicks a search result. When this option is not selected, the document is opened outside SharePoint in the corresponding Microsoft Office application.

b. In the **WebParts Content Indexing** section, you can select among four options to determine how the
connector indexes the content of Web Parts:

**Important:** Selecting to index dynamically generated content such as Web Parts may expose secured information as the crawler may see and index content that not all users have access to.

**Note:** Not all Web parts are available in Microsoft SharePoint Foundation 2010 (see Overview of Web Parts available in SharePoint Foundation 2010).

Don't index the WebParts content

Ignores the content of the Web Part pages, including the content of the Web Parts.

Index the content of all WebParts

Indexes the content of all Web Parts in all the Web Part pages. This option is not supported for SharePoint 2003.

Indexes the full WebPart page content, including menus

Indexes the complete Web Part pages as a web crawler would do. Because the full page is indexed, including menus, controls, etc., this option can cause index pollution.

Index the content of the WebParts of these types only

Only indexes the content of Web Parts which assembly types are listed in the text box appearing when the option is selected. The `Microsoft.SharePoint.WebPartPages.ContentEditorWebPart` type appears by default in the text box. This option is selected by default but is not supported for SharePoint 2003.

**Note:** You can find the assembly types of the Web Parts that you want to index from the **Site Settings** (see "Finding the Assembly Type of a SharePoint Web Part" on page 109).

c. In the **Server Name Alias** box, optionally enter a server name that, in the index, overrides the one from which documents are downloaded in the index. This parameter is useful to have query results point to a server other than the one used for indexing.

**Example:** Three network load balanced (NLB) SharePoint front-end servers handle the end-users requests and your source crawls a fourth mirror server to not impact performance for users. In the **Server Name Alias** box, enter the NLB URL to replace the IP address in the index.

d. In the **Priority** drop-down list, select the download priority relative to other SharePoint sources.

e. In the **Performance** section, consider disabling features to improve the performance:

**Disable advanced text layout analysis for PDF documents**

For better content indexing, CES by default analyzes PDF documents to identify text columns and restore appropriate content ordering. This process can be disabled to save CPU resources while indexing.

**Disable advanced duplicate document filtering**

By default CES applies an advanced filter to display only one copy of each document in the search
results. Select this option to disable the filtering of duplicate documents in order to save CPU resources and speed up indexing.

f. In the Conversion Timeout box, enter the number of minutes after which the converter proceeds to another document even if the conversion is not complete. When the timeout occurs, the document for which the conversion was aborted is considered corrupted. By default, the conversion timeout is 10 minutes.

g. Click Apply Changes.

7. Start indexing the source by clicking Start or Rebuild from the button bar at the top of the page.

8. Validate that the source building process is executed without errors:

   - In the navigation panel on the left, click Status, and then validate that the indexing proceeds without errors.

   OR

   - Open the CES Console to monitor the source building activities.

9.32.8 SharePoint Source Refresh Troubleshooting for the Legacy Connector

Deprecated

This topic presents possible causes and solutions for error messages logged by full or incremental refreshes on a Microsoft SharePoint source.

Unable to perform an incremental refresh of source [SourceName] from collection [CollectionName]. A full refresh is required before an incremental refresh can be performed.

No change token was found for the current web application.

Possible causes:

   - The source full refresh was stopped before the change token was persisted.

   - The source full refresh was unable to persist the change token (see "Unable to persist the incremental refresh token for source [SourceName] from collection [CollectionName]. Error:... " on page 1358).

   - The client has changed the source starting addresses, thus the change token is no more valid.

Possible solution:

   - Perform a full refresh of the source.

The last refresh of the source [SourceName] from collection [CollectionName] was not performed recently (30 days ago). Consider performing a full refresh of the source.

The change token is very old, which has two possible consequences:

   - The SharePoint web services might refuse to send modified data because it may contain too much information.

   - The incremental refresh run might be very long, thus it may be more efficient to perform a simple full refresh.
Possible solution:

- Perform a full refresh of the source

Unable to persist the incremental refresh token for source [SourceName] from collection [CollectionName].

Error:

An internal error is preventing the crawler to persist the change token, thus the incremental refresh run will not be possible.

Possible solution:

- Contact Coveo Support for more information.

9.33 OpenText Content Server Connector

CES 7.0.5388+ (April 2013)

The Coveo connector for OpenText Content Server (OTCS) allows you to crawl and bring OTCS content into the unified index, making it easily searchable by end-users.

Note: OpenText Content Server is a technology component that was formerly known as Livelink ECM - Enterprise Server (see the OpenText document Livelink is Now Part of the OpenText ECM Suite).

Connector Features

Content indexing

The connector can retrieve and index exclusively the following default OTCS entity types:

- Appearance Workspace Folder
- Appearance
- Category
- Channel
- Collection (without the children documents)
- Compound Document
- Discussion
- Document
- Enterprise Workspace
- Folder
- Live Report
- News
- Poll
Fully supported security model

The connector fully supports the OTCS security model using a security provider to get permissions for each indexed OTCS item. This means that, in Coveo search interfaces, a user searching for OTCS content only sees the content to which he has access in OTCS.

Incremental refresh CES 7.0.5425+ (May 2013)

The incremental refresh feature continuously and automatically refreshes indexed OTCS items as they are modified.
Notes:

- **CES 7.0.8541+ (September 2016)** The incremental refresh can take account of deleted items (except news items) that are stored in the Recycle Bin module.

A source full refresh or rebuild is required to update deleted news items since news are not in the Recycle Bin once deleted.

- Incremental refresh limitations:
  
  - A source full refresh or rebuild is required to update added and modified items in projects, channels, discussions, and task lists (child items).
  
  - A source full refresh or rebuild is required to update child items permissions when the parent item is modified.
  
  - Takes into account deleted items only if the OpenText Content Server Recycle Bin module is enabled in OTCS, but with **CES 7.0.8047–(Dec 2015)**, a source full refresh or rebuild is required to remove deleted items.

  - **CES 7.0.8388+ (June 2016)** Incremental refreshes are supported even if the Document Undelete module is not installed. However, when the module is not installed, deleted items (except documents) are not taken into account.

  - Not available for Livelink 9.7.1 sources.

Connector Feature History

<table>
<thead>
<tr>
<th>Coveo Platform version</th>
<th>Monthly release</th>
<th>Features</th>
</tr>
</thead>
<tbody>
<tr>
<td>7.0.9434</td>
<td>December 2018</td>
<td>Add support for OTCS 16 and 16.2</td>
</tr>
<tr>
<td>7.0.8225</td>
<td>March 2016</td>
<td>Add support for OTCS 10.5</td>
</tr>
</tbody>
</table>
| 7.0.5425              | May 2013        | - Add incremental refresh for OTCS  
|                       |                 | - Add support for Livelink 9.7.1 |
| 7.0.5388              | April 2013      | Introduction of the connector |

What's Next?

Review the deployment process (see "OpenText Content Server Connector Deployment Overview" on page 1360).

9.33.1 OpenText Content Server Connector Deployment Overview

The following procedure outlines the steps needed to deploy the OpenText Content Server (OTCS) connector. The steps indicate the order in which you must perform configuration tasks on both the OTCS and Coveo servers.
To deploy the OpenText Content Server connector

1. Validate that your environment meets the requirements (see "OpenText Content Server Connector Requirements" on page 1362).

2. In OpenText Content Server:
   a. Enable the Web Services.
      The Coveo connector requires OTCS Web services to operate. You must ensure that these Web services are available (see "Enabling the OpenText Content Server Web Services" on page 1362).
   b. Select or create the crawling account.
      The Coveo connector needs an OTCS account with which it can fully crawl the OTCS content (see "Setting Up an OpenText Content Server Crawling Account" on page 1365).

3. In the Coveo Administration Tool:
   a. Configure a user identity.
      The Coveo connector needs to know the OTCS account that you previously selected or created. You must create a CES user identity to use this account. Use either the Screen Name or the Email Address of the dedicated OTCS account. You will later assign this user identity to the security provider and the source used by the connector to crawl the OTCS content.
   b. Configure a security provider.
      The Coveo connector needs a security provider to be able to get the permissions for each indexed OTCS item, and therefore fully support the OTCS security model (see "Configuring an OpenText Content Server Security Provider" on page 1367).
   c. Configure and index the OpenText Content Server source.
      The Coveo connector needs to know details about OTCS to be able to index its content (see "Configuring and Indexing an OpenText Content Server Source" on page 1370).

4. Enrich your OTCS indexed content
   a. Optionally, create and use a mapping file to fine-tune indexed content
      Consider customizing the connector mapping file to fine-tune the indexed content or to index other entities in your OTCS (see "Creating an OpenText Content Server Connector Mapping File" on page 1376).
   b. Optionally, modify hidden source parameters.
      Once your OTCS source is up and running, if you encounter issues, consider modifying some hidden source parameters to try resolving the issues (see "Modifying Hidden OpenText Content Server Source Parameters" on page 1377).

5. Customize your search interfaces with OTCS content
a. Add OTCS facets to your search interfaces

You can create facets using fields such as the OTCSFileTypeName metadata to allow users to easily filter OTCS documents (see "Managing Built-in Facets and Related Results Appearing in a .NET Search Interface" on page 574).

b. Allow OTCS users to be authenticated in a Coveo search interface

When your OTCS is not integrated with Active Directory, your end-users need to sign in to OTCS in a Coveo search interface to be able to see search results from OTCS. In this case, you need to add the OTCS security provider to your search interface to allow end-user to sign in to OTCS (see "Adding Security Providers to a .NET Search Interface" on page 631).

9.3.3.2 OpenText Content Server Connector Requirements

Your environment must meet the following requirements to be able to use the Coveo connector for OpenText Content Server:

- **CES 7.0.5388+ (April 2013)**

- Coveo license for the OpenText Content Server connector

  - Your Coveo license must include support for the OpenText Content Server connector to be able to use this connector.

- OpenText product support:

  - OpenText Content Server (OTCS) 16 or 16.2
  - Deprecated support versions: Livelink 9.7.1 **CES 7.0.5425+ (May 2013)**, and OTCS 10 and 10.5

What's Next?

The Coveo connector for OpenText Content Server (OTCS) needs OpenText Web services to be able to index OTCS content (see "Enabling the OpenText Content Server Web Services" on page 1362).

9.3.3.3 Enabling the OpenText Content Server Web Services

The Coveo connector for OpenText Content Server (OTCS) needs OpenText Web services to be able to index OTCS content. The files for the required web services are installed with the OTCS installation.

Use the following procedures to correctly connect, configure, and set permissions for OTCS Web services:

- "Connecting the OTCS Web Services" on page 1362
- "Setting IIS Permissions" on page 1364
- "Enabling WCF Services" on page 1365

9.3.3.3.1 Connecting the OTCS Web Services

1. Using an administrator account, connect to your OTCS server.

2. Start **Internet Information Services (IIS) Manager**.
3. On the Internet Information Services (IIS) Manager left pane, expand your server > Sites.

4. If not already done when you installed OTCS, right-click Default Web Site, and then select Add Application in the menu, and in the Add Application dialog box:

![Add Application dialog box](image)

   a. In the Alias box, enter les-services or cws (OTCS 10.5+).

   b. In the Physical path box, enter C:\OPENTEXT\webservices\dotnet\les-services or C:\OPENTEXT\webservices\dotnet\cws (OTCS 10.5+).

   c. Click OK.

Note: The Coveo connector needs the following OTCS web services that are installed by default in the C:\OPENTEXT\webservices\dotnet\les-services (C:\OPENTEXT\webservices\dotnet\cws for OTCS 10.5+) folder:

- Authentication
- DocumentManagement
- IndexService
- MemberService
- ContentService

5. Back on the Internet Information Services (IIS) Manager left pane, click your new les-services or cws (OTCS 10.5+) application.
6. On the right pane, click Advanced Settings and in the Advanced Settings dialog box:
   a. In Application Pool, select ASP.NET 2.0.
   b. Click OK.

7. Still with new les-services or cws (OTCS 10.5+) application selected, in the central pane, double-click Handler Mappings.

8. On the right pane, click Edit Feature Permissions and in the Edit Feature Permissions dialog box:
   a. Select the Read and Script check boxes.
   b. Click OK.

9.33.3.2 Setting IIS Permissions

1. On the OTCS server, using Windows Explorer, navigate to the [OT_HOME]\webservices\dotnet folder.

2. Right-click the les-services or cws (OTCS 10.5+) folder, and then choose Properties.

3. In the les-services Properties or cws Properties (OTCS 10.5+) dialog box:
   a. Select the Security tab.
   b. Under Group or user names, click Edit.
   c. In the Permissions for les-services or Permissions for cws (OTCS 10.5+) dialog box:
      i. Add the local IUSR user with the Read permissions.
      ii. Add the IIS Application Pool Identity (e.g. ApplicationPoolIdentity or NetworkService) with Read & execute permission.
      iii. Click OK.
   d. Click OK.

4. In the Windows Explorer, open the [OT_HOME]\webservices\dotnet\les-services or [OT_HOME]\webservices\dotnet\cws (OTCS 10.5+) folder.

5. Right-click the logs folder, and then choose Properties.

6. In the logs Properties dialog box:
   a. Select the Security tab.
   b. Under Group or user names, click Edit.
   c. In the Permissions for logs dialog box:
      i. For the IIS Application Pool Identity (e.g. ApplicationPoolIdentity or NetworkService) select the Modify permission.
ii. Click **OK**.

d. Click **OK**.

9.33.3.3 Enabling WCF Services

1. On the OTCS server, open a **Command Prompt** window (cmd.exe).

2. Execute the following command to enable the WCF Services:
   
   "%SystemRoot%\Microsoft.NET\Framework\v3.0\Windows Communication Foundation\ServiceModelReg.exe" -i

3. When the command completes, close the **Command Prompt** window.

What's Next?

Select or create an OTCS crawling account to be used by the Coveo connector to fully crawl the OTCS content (see "Setting Up an OpenText Content Server Crawling Account" on page 1365).

9.33.4 Setting Up an OpenText Content Server Crawling Account

The Coveo connector needs to connect to the OpenText Content Server (OTCS) using an account that has read access to all the OTCS content that you want to index. The Coveo connector only reads and does not modify the OTCS content.

The best practice is to create an OTCS crawling account with a non-expiring password to be used exclusively by the Coveo connector and grant this account complete read access to all OTCS content. When you want to also index permissions, the crawling account requires **System administration rights**.

To grant the crawling account read permissions to all items

1. Using an administrator account, sign in to **OpenText ECM Suite**.

2. On the **OpenText Content Server** menu, select **Enterprise > Workspace**.

3. Next to **Enterprise**, click the Functions arrow, and in the menu, select **Permissions**.
4. In the Permissions page:

   a. In the Assigned Access section, add the crawling account to which you want to grant the rights.

   b. Click the newly created crawling account, and in the Edit User Permissions pane:
      
      i. Select the See Contents check box.

      ii. In the Apply To drop-down list, select This item & sub-items.

      iii. In the Sub-Items Options, select the check boxes for item types that you want to index.

      iv. Click Update.

To grant the crawling account System Administration Rights

1. Using an administrator account, sign in to OpenText ECM Suite.

2. On the OpenText Content Server menu, select Enterprise > Users & Groups.
3. In the **Users and Groups** page, find the user to which you want to grant Administration rights, and then click the **Edit** link for that user.

4. In the **General Info for: [username]** page:
   
   a. Select the **General** tab.
   
   b. In the **Privileges** section at the bottom, select the **System administration rights** check box.
   
   c. Click **Update**.

**What's Next?**

On the Coveo server, configure a CES user identity for your OTCS crawling account and then create a security provider (see "Configuring an OpenText Content Server Security Provider" on page 1367).

**9.33.5 Configuring an OpenText Content Server Security Provider**

The Coveo connector needs a security provider to be able to get the permissions for each indexed OpenText Content Server (OTCS) item, and therefore fully support the OTCS security model. This means that, in a Coveo
search interface, a user searching for OTCS content only sees the content to which he has access in OTCS.

Note: You can get familiar with how Coveo components deal with permissions on documents both at indexing and query time.

To configure a OpenText Content Server security provider

1. On the Coveo server, access the Administration Tool.
3. In the Security page, in the navigation panel on the left, click Security Providers.
4. In the Security Providers page, click Add to create a new security provider.
5. In the Modify Security Provider page:

   a. In the Name box, enter a name to identify this security provider.

      Example: OpenText Content Server Security Provider

      Note: You can also use the OTCS connector to crawl a Livelink version 9.7.1 source. You need to add a hidden parameter to do so (see below).
b. In the **Security Provider Type** drop-down list, select **OpenText Content Server (x64)**.

c. In the **User Identity** section:
   i. In the drop-down list, select the user identity that you selected or created previously.
   ii. When needed, click **Add**, **Edit**, or **Manage user identities** respectively to create, modify, or manage user identities.

d. **CES 7.0.5556+ (June 2013)** In the **Security Provider for User Mappings** drop-down list, select the security provider that will receive the login names of the users and perform the mapping to OTCS users.

   **Example:** When Microsoft Windows users perform a search, select an **Active Directory** security provider to map AD users to OTCS users.

e. In the **Web Service Url** box, enter the address of the OpenText Content Server Web Service. By default, this value is:

   http://OTCS_Server/les-services/

   where you replace **OTCS_Server** by the fully qualified domain name of your server.

   **Example:** http://OTCS.corp.MyCompany.com/les-services/

   **Important:** **CES 7.0.8225+ (March 2016)** *(For OTCS 10.5+ only)* Replace **les-services** by **cws**.

   **Example:** http://OTCS.corp.MyCompany.com/cws/

   **Note:** You will also need to specify this URL in the **Web Service URL** parameter when you configure your source (see "Configuring and Indexing an OpenText Content Server Source" on page 1370).

f. In the **Web Service Configuration File** box, in rare cases where the security provider encounters communication issues with Windows Communication Foundation (WCF), you can modify the way in which the security provider communicates with OTCS by entering the path and file name of a custom configuration file (see the Microsoft document **Configuring Services Using Configuration Files**).

g. Next to **Parameters**, click **Add Parameter** when you want to show and use advanced source parameters (see "Modifying Hidden OpenText Content Server Source Parameters" on page 1377).

   **Important:** **CES 7.0.5425+ (May 2013)** When you are indexing a Livelink v9.7.1, you must add the **OTCSVersion** parameter and enter the **9.7.1** value.

h. Leave the **Allow Complex Identities** option cleared as it does not apply to this type of security provider.

   i. Click **Apply Changes**.

What’s Next?

Configure and index an OTCS source (see "Configuring and Indexing an OpenText Content Server Source" on page 1370).
9.33.6 Configuring and Indexing an OpenText Content Server Source

A source defines a set of configuration parameters for a specific OpenText Content Server (OTCS).

**Note:** In an environment with more than one OTCS, you need to define one source for each OTCS that you want to index.

To configure and index an OpenText Content Server source

1. On the Coveo server, access the Administration Tool.
2. Select Index > Sources and Collections.
3. In the Collections section:
   a. Select an existing collection in which you want to add the new source.
   OR
   b. Click Add to create a new collection.
4. In the Sources section, click Add.

The Add Source page that appears is organized in three sections.

5. In the General Settings section of the Add Source page:
a. Enter the appropriate value for the following required parameters:

**Name**

Enter a descriptive name of your choice for the connector source.

**Example:** OpenText Content Server

**Source Type**

Select the connector used by this source. In this case, select OpenText Content Server.

**Notes:** If you do not see OpenText Content Server, your environment does not meet the requirements (see "OpenText Content Server Connector Requirements" on page 1362).

You can also use the OTCS connector to crawl a Livelink version 9.7.1 source. You need to add a hidden parameter to do so (see below).

**Addresses**

Enter the document or folder IDs that you want to index. One ID per line or * to index the whole OTCS content from the Enterprise Workspace root.

**Note:** CES 7.0.6830—(July 2014) This parameter is not used for the OpenText Content Server connector, but must not be left empty. Enter NA.

You can also find the ID for a node in OTCS by clicking the Functions icon of an item, selecting Properties > General on the menu, clicking Change next to Nickname, and then read the Item ID value.

**Example:** When you want to create an OTCS source only for one project, in the project General property tab, read the Item ID value, like 4094 in the following example.
Note: Using certain item types as the root node will result in an error when retrieving their permissions. All item types receiving their permissions from their parents (such as Task, News, all types under Discussion, and possibly other types) are not supported as the root node.

Refresh Schedule

Time interval at which the source is automatically refreshed to keep the index content up-to-date. The recommended Every day option instructs CES to refresh the source everyday at 12 AM.

Note: You can create new or modify existing source refresh schedules.

b. Review the value for the following parameters that often do not need to be modified:

Rating

Change this value only when you want to globally change the rating associated with all items in this source relative to the rating to other sources.

Example: When a source replaces a legacy system, you may want to set this parameter to High, so that in the search interface, results from this source appear earlier in the list compared to those from legacy system sources.

Document Types

If you defined a custom document type set for this source, select it.

Active Languages

If you defined custom active language sets, ensure to select the most appropriate for this source.

Fields

By default, when an OTCS metadata name matches the name of a CES standard or custom field, the metadata value is automatically mapped to the CES field and the field can be used to make the search interface results more relevant. It is a good practice to create a custom field set that and fields with names matching those of your signification OTCS metadata.

If you defined custom field sets, ensure to select the most appropriate for this source.

6. In the Specific Connector Parameters & Options section of the Add Source page:
a. Configure the following required parameters:

**Web Service URL**

Enter the URL of the OpenText Content Server Web Service used to communicate with the server. By default, this value is:

http://OTCS_Server/les-services/

where you replace `OTCS_Server` by the fully qualified domain name of your server.

**Example:** http://OTCS.corp.MyCompany.com/les-services/

**Important:** CES 7.0.8225+ (March 2016) (For OTCS 10.5+ only) Replace les-services by cws.

**Example:** http://OTCS.corp.MyCompany.com/cws/

**Note:** This is the same value that you entered for the Web Service URL parameter when you configured the security provider (see "Configuring an OpenText Content Server Security Provider" on page 1367).

**Content Server URL**

Enter the URL pointing to the OpenText Content Server necessary to have valid clickable URIs.

**Example:** When you access the OTCS, the Content Server URL is the part of the URL before Livelink.exe:

In the above example: http://OTCS.corp.MyCompany.com/OTCS/
b. Review the value for the following parameters that often do not need to be modified:

**Mapping File**

By default, when an OTCS metadata name matches the name of a CES standard or custom field, the metadata value is automatically mapped to the CES field. When this default behavior is sufficient to leverage OTCS metadata, leave this field empty.

When you want to control more precisely how to map OTCS metadata to CES fields, create a custom mapping file and enter the absolute full path pointing to your file (see "Creating an OpenText Content Server Connector Mapping File" on page 1376).

Example: `C:\CES\Config\MyOTCSMappingFile.xml`

**Number of Refresh Threads**

Enter the number of threads that will be used to retrieve OpenText Content Server content. The default value is 2.

**Parameters**

Click **Add Parameter** when you want to show and use advanced source parameters (see "Modifying Hidden OpenText Content Server Source Parameters" on page 1377).

**Important:** CES 7.0.5425+ (May 2013) When you are indexing a Livelink v9.7.1, you must add the OTCSVersion parameter and enter the 9.7.1 value.

c. In the **Option** section:

**Index Subfolders**

Keep this check box selected (recommended). By doing so, all subfolders from the specified portal address are indexed.

**Index the document's metadata**

When selected, CES indexes all the document metadata, even metadata that are not associated with a field. The orphan metadata are added to the body of the document so that they can be searched using free text queries.

When cleared (default), only the values of system and custom fields that have the **Free Text Queries** attribute selected will be searchable without using a field query.
Example: A document has two metadata:

- LastEditedBy containing the value Hector Smith
- Department containing the value RH

In CES, the custom field CorpDepartment is bound to the metadata Department and its Free Text Queries attribute is selected.

When the **Index the document's metadata** option is cleared, searching for RH returns the document because a field is indexing this value. Searching for hector does not return the document because no field is indexing this value.

When the **Index the document's metadata** option is selected, searching for hector also returns the document because CES indexed orphan metadata.

Document's addresses are case-sensitive

Leave the check box cleared. This parameter needs to be checked only in rare cases for systems in which distinct documents may have the same name but different casing.

Generate a cached HTML version of indexed documents

When you select this check box (recommended), at indexing time, CES creates HTML versions of indexed documents. In the search interfaces, users can then more rapidly review the content by clicking the **Quick View** link rather than opening the original document with the original application. Consider clearing this check box only when you do not want to use **Quick View** links or to save resources when building the source.

Open results with cached version

Leave this check box cleared (recommended) so that in the search interfaces, the main search result link opens the original document with the original application. Consider selecting this check box only when you do not want users to be able to open the original document but only see the HTML version of the document as a **Quick View**. In this case, you must also select **Generate a cached HTML version of indexed documents**.

7. In the **Security** section of the **Add Source** page:
a. In the **OpenText Content Server Security Provider** drop-down list, select the security provider that you created for this source (see "Configuring an OpenText Content Server Security Provider" on page 1367).

b. In the **Authentication** drop-down list, select the user identity that you created for the OpenText Content Server.

c. Click **Save and Start** to save the source configuration and start indexing this source.

8. Validate that the source building process is executed without errors:

   - In the navigation panel on the left, click **Status**, and then validate that the indexing proceeds without errors.

   OR

   - Open the CES Console to monitor the source building activities.

**What's Next?**

Set an incremental refresh schedule for your source.

If you experience issues or want to fine tune how your OTCS source is indexed, consider using hidden OTCS source parameters (see "Modifying Hidden OpenText Content Server Source Parameters" on page 1377).

9.33.6.1 Creating an OpenText Content Server Connector Mapping File

The Coveo connector for OpenText Content Server (OTCS) has no mapping file by default. When the name of metadata found on OTCS documents matches the name of CES system or custom fields, the metadata are automatically mapped.

When you need to more accurately control where and how metadata is mapped on your items, you must create and use a mapping file that respects the schema of the standard mapping file (see "Standard Mapping File Schema" on page 58).

**Examples:** You need a mapping when you want to:

- Customize the HTML body for items of a specific type.
- Concatenate two or more OTCS metadata in a CES field.
- Map an OTCS metadata value to a CES field for which names do not match.

To create and use an OTCS connector mapping file

1. Using an administrator account, connect to the Coveo Master server.

2. Using a text editor:

   a. Create the mapping file.

   You can start with the following commented sample mapping file.

```xml
<xml version="1.0" encoding="utf-8" ?>
<Mappings>!-- Review the ValidationschemaVersion1.xsd to view the available fields and attributes -->
```
b. Respecting the mapping file format, customize the file using the following tips:

- Use OTCS node types to create specific `<Mapping type="...">` tags in the mapping file.

  You can easily find the values to enter in this tag from the Type of items in OpenText Content Server.

  **Example:** When you want to manage OTCS Discussion fields, in the OTCS Workspace, simply hover a discussion item. The tooltip indicates the value to enter in the Mapping type tag.

  ![Discussion Tooltip](image)

  In the mapping file, you would create the `<Mapping type="Discussion">` node.

- The connector populates the special OTCSFileType metadata with the type of OTCS documents. This metadata is useful to create a facet based on the types of items found in OTCS.

c. Save the file using a name of your choice in the [Index_Path]\Config\ folder.

d. Save your changes.

What's Next?

Assign your customized mapping file in your OpenText Content Server source (see "Configuring and Indexing an OpenText Content Server Source" on page 1370).

9.33.6.2 Modifying Hidden OpenText Content Server Source Parameters

The Add Source and Source: ... General pages of the Administration Tool present the parameters with which you can configure the connector for most OpenText Content Server (OTCS) setups. More advanced and more rarely used parameters are hidden. You can choose to make one or more of these parameters appear in the Add Source and Source: ... General pages of the Administration Tool so that you can change their default value. Consider changing values of hidden parameters when you encounter issues.
The following list describes the advanced hidden parameters available with OTCS sources. The parameter type (integer, string...) appears between parentheses following the parameter name.

**SpecificContentDeletionNode (String)** CES 7.0.8541+ (September 2016)

This ID of the node enabled on the OTCS server used for the content deletion process. The parameter value can either be an UndeleteWS or a Recycle Bin node ID. The default value is -1, which tells the connector to ignore the parameter.

**Notes:**

- When available, you find the Recycle Bin node ID after objID= in the Content Server URL.

**Example:** In the following OpenText Content Server URL, the Recycle Bin node ID is 126020:

http://<OTCSServer>/OTCS/livelink.exe?func=ll&objId=126020=&objAction=browse

- The parameter is necessary when the connector cannot automatically detect the UndeleteWS node or Recycle Bin ID, which is necessary to take account of deleted items during incremental refreshes.

**TreatPublicAccessAsAnonymous (Boolean)** CES 7.0.8541+ (September 2016)

Whether to add anonymous access if "public access" is specified on the content object. The default value is False.

**UseOtcsContentTypes (Boolean)** CES 7.0.8388+ (June 2016)

Whether to use the content types returned by OTCS instead of "binary file". The default value is False.

**Note:** When you set the parameter value to True, update the document type set used by your OTCS source to ensure all content types returned by OTCS are indexed.

**Example:** When you want to index all Microsoft Office 2007+ documents (Word, Excel, and PowerPoint), ensure the following document types are contained in the document set used by the source: .doc, .docx, .dot, .dotx, .dotm, .dotm, .xls, .xlt, .xla, .xlsx, .xltx, .xlsm, .xltx, .xltd, .xlam, .xlab, .ppt, .pot, .pps, .ppa, .pptx, .potx, .ppsx, .potx, .ppam, .pptm, .potm, .ppsm

**BatchSize (Integer)**

Number of items to fetch per request made to the OTCS. The default value is 256. The minimum value is 1. A small value forces the connector to make small but frequent queries to OTCS. A larger value leads to larger and less frequent queries.

**WebServiceConfigFile (String)**

The path and file name of a custom configuration file. In rare cases where the connector encounters communication issues with Windows Communication Foundation (WCF), you can modify the way in which the connector communicates with OTCS by creating and specifying a custom configuration file (see the Microsoft document Configuring Services Using Configuration Files).
**ItemTypesToIndex (String)**

By default, this parameter is empty so that all supported OTCS item types are indexed. You can use this parameter to restrict the types of OTCS items to be indexed by entering only the OTCS item types that you want to index, separated by a semi-colon ;. You can easily find the values to enter in this parameter from the **Type** of items in OpenText Content Server. In the OTCS Workspace, simply hover a discussion item. The tooltip indicates the value to enter in the parameter.

**SpecificRootNode (Integer) (deprecated)** CES 7.0.6830– (July 2014)

**Note:** CES 7.0.6942+ (August 2014) The **Addresses** parameter replaces it (see Configuring and Indexing an OpenText Content Server Source).

By default, the connector crawls the whole OTCS content from the Enterprise Workspace root. You can use this parameter to specify to start crawling from another root node or from a subnode by entering the node ID.

You can find this ID for a node in OTCS by clicking the Functions icon of an item, selecting **Properties > General** on the menu, clicking **Change** next to **Nickname**, and then reading the **Item ID** value.

**Example:** When you want to create an OTCS source only for one project, in the project **General** property tab, read the **Item ID** value, like **4094** in the following example.

**Note:** Using certain item types as the root node will result in an error when retrieving their permissions. All item types receiving their permissions from their parents (such as **Task**, **News**, all types under **Discussion**, and possibly other types) are not supported as the root node.
**NumberOfRefreshThreads (Integer)**

This parameter determines the number of threads used to simultaneously crawl OTCS. The default value is 1.

**RetrieveFullNodeData (Boolean)**

By default this parameter is set to True to instruct the connector to perform additional OTCS requests to extract all node metadata and allow to get the OTCS Category data. When you do not want to index OTCS Category data, set this parameter to False to roughly double the crawling speed.

**OTCSVersion (String)**  
**CES 7.0.5425+ (May 2013)**

This parameter allows to specify the version of the OTCS/Livelink source to crawl. You need to add this parameter only when you want to crawl a Livelink version 9.7.1 source. The two possible values are:

- 10sp2 - The default to crawl an OpenText Content Server source.
- 9.7.1 - To crawl a Livelink source.

**RetrieveUsers (Boolean)**  
**CES 7.0.5785+ (August 2013)**

When set to True, this parameter instructs the connector to retrieve the OTCS users. The default value is False.

**Example:** When the authors of OTCS documents are user IDs, not the user names, set the RetrieveUsers parameter to True to retrieve the users. You can then map the user IDs to the user names so that in the search results, you can display user names rather than user IDs.

To modify hidden OpenText Content Server source parameters:

1. Refer to "Adding an Explicit Connector Parameter" on page 450 to add one or more OpenText Content Server hidden source parameters.

2. For a new OpenText Content Server source, access the Add Source page of the Administration Tool to modify the value of the newly added advanced parameter:
   a. Select Index > Sources and Collections.
   b. Under Collections, select the collection in which you want to add the source.
   c. Under Sources, click Add.
   d. In the Add Source page, edit the newly added advanced parameter value.

3. For an existing OpenText Content Server source, access the Source: ... General page of the Administration Tool to modify the value of the newly added advanced parameter:
   a. Select Index > Sources and Collections.
   b. Under Collections, select the collection containing the source you want to modify.
   c. Under Sources, click the existing OpenText Content Server source in which you want to modify the newly added advanced parameter.
   d. In the Source: ... General page, edit the newly added advanced parameter value.

4. Rebuild your OpenText Content Server source to apply the changes to the parameters.
9.34 Oracle Knowledge Connector

CES 7.0.7256+ (December 2014)

The Coveo connector for Oracle Knowledge (formerly known as InQuira Knowledge Management) allows you to index and integrate the content of your Oracle Knowledge instance into your Coveo unified index, making it easily searchable by end-users.

9.34.1 Features

- Content Indexing
  
  Retrieval and indexing of the following Oracle Knowledge items:
  
  - Content channel
  - Content record
  - Content record attachment
  - Discussion board
  - Forum
  - Topics and messages

  **Note:** The attachments of the topics and messages are not retrievable by the Oracle Knowledge APIs.

- Security

  The connector supports Oracle Knowledge security model by indexing Oracle Knowledge item permissions so that in Coveo search interfaces, a user searching Oracle Knowledge content only sees the content to which he has access in Oracle Knowledge.

- Pause/Resume

  When indexing an Oracle Knowledge instance, the connector can be paused and resumed.

- Partial Incremental Refresh

  Updated documents in a repository (content/security) are periodically re-indexed by the connector (see "Configuring and Indexing an Oracle Knowledge Source" on page 1386).

  **Note:** Some deleted and unpublished items require a full refresh to be taken in account (see "Limitation" on page 1381).

9.34.2 Limitation

- Limited incremental refresh capabilities:
  
  - A full refresh is needed to update deleted items
  - A full refresh is needed to update changes on unpublished content records
What's Next?

Get familiar with the connector deployment steps (see "Oracle Knowledge Connector Deployment Overview" on page 1382).

9.34.3 Oracle Knowledge Connector Deployment Overview

The following procedure outlines the steps needed to deploy the Oracle Knowledge connector. The steps indicate the order in which you must perform configuration tasks on both the Oracle Knowledge and Coveo servers.

To deploy the Oracle Knowledge connector

1. Validate that your environment meets the requirements (see "Oracle Knowledge Connector Requirements" on page 1383).

2. On the Oracle Knowledge instance, create a Knowledge Administrator user to be used as a crawling account (see Create a Knowledge Administrator).

3. On the machine hosting Oracle Knowledge, copy the IQServiceClientCS.dll file located in the MSFT folder.

   Example: C:\Oracle\Knowledge\IM\InfoManager\clientLibrary\MSFT\Release

4. On the machine hosting CES, paste the IQServiceClientCS.dll file in the Bin folder of CES.

   Example: C:\Program Files\Coveo Enterprise Search 7\Bin

5. On the Coveo server:

   a. Create a user identity.

      The connector needs an account that has at least read access to all item types and security permissions of the Oracle Knowledge instance. Create a CES user identity that must contain the credentials (username and password) of a console user with one or more security roles (custom or built-in) allowing him to view all content and permissions of the Information Manager repository you want to index (see "Adding a User Identity" on page 420).

   b. (Optional) Create security providers

      When you want to index Oracle Knowledge permissions, you must create two security providers to get Oracle Knowledge item permissions and resolve and expand groups.

      In Oracle Knowledge, users are identified by their email addresses. Consequently, permissions returned by the Oracle Knowledge security provider for each item are email addresses. The Oracle Knowledge security provider then requires another security provider to uniquely identify users from their email addresses.

      i. Start by selecting or creating an Email or an Active Directory security provider that the Oracle Knowledge security provider will use to resolve and expand groups. The security provider type to use depends on how users are authenticated when they access the search interface:
When authenticated with their email address, use an Email security provider (see "Configuring an Email Security Provider" on page 65).

When authenticated with an Active Directory account, use an Active Directory security provider (see "Configuring an Active Directory Security Provider" on page 1141).

Notes:

- CES comes with an Active Directory security provider that you can configure to connect to the default domain. When your environment contains more than one domain, you can select an Active Directory security provider that you created for other domains.

- An Active Directory security provider is appropriate only when the User Principal Name (UPN) matches the email address for all users.

Note: You may require to also use a REGEX Transform Member Name security provider in between the two other security providers to map member types. Contact Coveo Support for assistance.

ii. Then create an Oracle Knowledge security provider that the connector uses to resolve indexed permissions (see "Configuring an Oracle Knowledge Security Provider" on page 1384).

c. Create an Oracle Knowledge field set.

   It is recommended to import the out-of-the-box Oracle Knowledge field set ([CES_Path]\Bin\Coveo.CES.CustomCrawlers.OracleKnowledge.FieldSet.xml) to be able to easily add Oracle Knowledge specific facets to your Coveo search interfaces.

d. Configure and index the Oracle Knowledge source.

   The Coveo connector needs to know details about your Oracle Knowledge instance to be able to index its content (see "Configuring and Indexing an Oracle Knowledge Source" on page 1386).

9.34.4 Oracle Knowledge Connector Requirements

Your environment must meet the following requirements to be able to use the Coveo connector for Oracle Knowledge:

- CES 7.0.7256+ (December 2014)

- Coveo license for the Oracle Knowledge connector

  Your Coveo license must include support for the Oracle Knowledge connector to be able to use this connector.

- Supported Oracle Knowledge version

  The connector supports Oracle Knowledge 8.4.2.2 to 8.5.1 installations.

What's Next?

Review the deployment process (see "Oracle Knowledge Connector Deployment Overview" on page 1382).
9.34.5 Configuring an Oracle Knowledge Security Provider

When you choose to index permissions associated with Oracle Knowledge items, the Coveo connector needs a security provider. When permissions are indexed, in Coveo search results, a user searching for Oracle Knowledge content only sees the content to which he has access in Oracle Knowledge.

**Note:** You can get familiar with how Coveo components deal with permissions on documents both at indexing and query time.

To configure an Oracle Knowledge security provider:

1. On the Coveo server, access the Administration Tool.
2. Select **Configuration > Security**.
3. In the navigation panel on the left, click **Security Providers**.
4. In the **Security Providers** page, click **Add** to create a new security provider.
5. In the **Modify Security Provider** page:
a. Configure the following required parameters:

**Name**
Choose a significant name to identify the security provider.

*Example:* Oracle Knowledge Security Provider

**Security Provider Type**
Select *Oracle Knowledge (x64).*

**User Identity**
Select the Oracle Knowledge user identity that you created previously.

**The Oracle Knowledge server URL**
Enter the URL to the client API web service.

The connector auto-filled this URL with /imws/WebObjects/imws.woa/ws/RequestProcessor.

**The Oracle Knowledge repository name**
Enter the name of the Information Manager repository to index.

*Note:* The repository name is the same value that you enter in the Repository box when you log in to your Oracle Knowledge Information Manager.

**Security Provider**
When you want to index Oracle Knowledge security permissions, select the security provider that you selected or created to allow this security provider to resolve and expand the groups (see *Oracle Knowledge Connector Deployment Overview*).

b. Review the default value of the following check box:

**Whether to treat a banned user as inactive**
Whether to treat a banned user as inactive. By default, banned users are treat as active.

c. Review if you need to change the default values for the following parameter:

**The Users and UserGroups cache expiration time**
Enter the time before a cached object is marked as expired and must be reindexed. The default value is 60 min.

d. Click *Add Parameter* when you want to show and change the value of advanced source parameters (see "Modifying Hidden Oracle Knowledge Source Parameters" on page 1392).

e. Leave the *Allow Complex Identities* cleared as it does not apply to this type of security provider.

f. Click *Apply Changes.*
What's Next?

Configure and index an Oracle Knowledge source (see "Configuring and Indexing an Oracle Knowledge Source" on page 1386).

9.34.6 Configuring and Indexing an Oracle Knowledge Source

A source defines a set of configuration parameters for a specific Oracle Knowledge instance. When you want to index more than one Information Manager repository, configure one source per repository.

To configure and index an Oracle Knowledge source

1. On the Coveo server, access the Administration Tool.
2. Select Index > Sources and Collections.
3. In the Collections section:
   a. Select an existing collection in which you want to add the new source.
   OR
   b. Click Add to create a new collection.
4. In the Sources section, click Add.
   The Add Source page that appears is organized in three sections.
5. In the General Settings section of the Add Source page:
a. Enter the appropriate value for the following required parameters:

**Name**

A descriptive name of your choice for the connector source.

*Example: Oracle Knowledge Employee Directory*

**Source Type**

The connector used by this source. In this case, select *Oracle Knowledge*.

*Note: If you do not see *Oracle Knowledge* in the Source Type list, ensure that your environment meets the requirements (see "Oracle Knowledge Connector Requirements" on page 1383).*

**Addresses**

Enter the base URL of your Oracle Knowledge server.

*Examples: http://MyOracleKnowledgeServer:8226/

*Important: The starting address specified here must match the one entered in the security provider configuration page (see Configuring an Oracle Knowledge Security Provider).*

**Fields**

Select the field set that you created earlier (see Oracle Knowledge Connector Deployment Overview).
b. The following parameters often do not need to be changed:

**Rating**

Change this value only when you want to globally change the rating associated with all items in this source relative to the rating of other sources.

*Example:* When the source indexes a legacy repository, you may want to set this parameter to *Low*, so that in the search interface, results from this source appear lower in the list compared to those from active repository sources.

**Document Types**

If you defined a custom document type set for this source, select it.

**Active Languages**

If you defined custom active language sets, ensure to select the most appropriate for this source.

**Refresh Schedule**

Time interval at which the index is automatically refreshed to keep the index content up-to-date. By default, the *Every day* option instructs CES to refresh the source everyday at 12 AM.

*Note:* The full refresh is a safety net to ensure all modifications are taken into account (see Oracle Knowledge Incremental Refresh Limitations).

6. In the **Specific Connector Parameters & Options** section of the **Add Source** page:

   ![Specific Connector Parameters & Options](image)

   a. Enter the appropriate value for the following required parameters:

   **Repository Name**

   Enter the name of the Information Manager repository to index.
Note: The repository name is the same value that you enter in the Repository box when you log in to you Oracle Knowledge Information Manager.

Example: Employee Directory

Important: The repository name specified must match the one entered in the security provider configuration page (see Configuring an Oracle Knowledge Security Provider).

Resource Host URL

Enter the root URL of the Oracle Knowledge server resources.

Example: http://MyOracleKnowledgeServer:8226/resources/

b. In the Mapping File box, the path to the default mapping file that defines how the connector handles metadata often does not need to be changed.

c. Review if you need to change the default values for the following options:

Index Unpublished Content Records

Whether to index the latest version of the content records, even if the version is unpublished. By default, only the latest published version is indexed.

Index Discussion Boards

Whether to index discussion boards. By default, discussion boards are indexed.

d. Click Add Parameter when you want to show and change the value of advanced source parameters (see "Modifying Hidden Oracle Knowledge Source Parameters" on page 1392).

e. The Option check boxes generally do not need to be changed:

Index Subfolders

Keep this check box selected (recommended). By doing so, all subfolders from the specified server address are indexed.

Index the document’s metadata

When selected, CES indexes all the document metadata, even metadata that are not associated with a field. The orphan metadata are added to the body of the document so that they can be searched using free text queries.

When cleared (default), only the values of system and custom fields that have the Free Text Queries attribute selected will be searchable without using a field query.
Example: A document has two metadata:
- LastEditedBy containing the value Hector Smith
- Department containing the value RH

In CES, the custom field CorpDepartment is bound to the metadata Department and its Free Text Queries attribute is selected.

When the Index the document's metadata option is cleared, searching for RH returns the document because a field is indexing this value. Searching for hector does not return the document because no field is indexing this value.

When the Index the document's metadata option is selected, searching for hector also returns the document because CES indexed orphan metadata.

Document's addresses are case-sensitive

Leave the check box cleared. This parameter needs to be checked only in rare cases for systems in which distinct documents may have the same name but different casing.

Generate a cached HTML version of indexed documents

When you select this check box (recommended), at indexing time, CES creates HTML versions of indexed documents. In the search interfaces, users can then more rapidly review the content by clicking the Quick View link rather than opening the original document with the original application. Consider clearing this check box only when you do not want to use Quick View links or to save resources when building the source.

Open results with cached version

Leave this check box cleared (recommended) so that in the search interfaces, the main search result link opens the original document with the original application. Consider selecting this check box only when you do not want users to be able to open the original document but only see the HTML version of the document as a Quick View. In this case, you must also select Generate a cached HTML version of indexed documents.

7. In the Security section of the Add Source page:
a. In the **Authentication** drop-down list, select the Oracle Knowledge crawling user identity that you created for this source (see Oracle Knowledge Connector Deployment Overview).

b. In the **Security Provider** drop-down list, if you chose to index permissions, select the Oracle Knowledge security provider that you created for this source (see "Configuring an Oracle Knowledge Security Provider" on page 1384). Otherwise, select **None**.

c. Click **Save** to save the source configuration.

8. In the case your Oracle Knowledge content is all public and you chose to not index Oracle Knowledge permissions:

   a. In the navigation menu on the left, select **Permissions**.
   
   b. Next to **Permissions**, select the **Specifies the security permissions to index** option.
   
   c. Next to **Allowed Users**, ensure that a well-known everyone group such as the Active Directory `everyone \S-1-1-0\` is added.
   
   d. Click **Apply Changes**.

9. Validate that the source building process is executed without errors:
In the navigation panel on the left, click **Status**, and then validate that the indexing proceeds without errors.

OR

Open the CES Console to monitor the source building activities.

What's Next?

Consider modifying advanced source parameters (see "Modifying Hidden Oracle Knowledge Source Parameters" on page 1392).

9.34.6.1 Modifying Hidden Oracle Knowledge Source Parameters

The **Add Source** and **Source: ... General** pages of the Administration Tool present the parameters with which you can configure the connector for most Oracle Knowledge setups. More advanced and more rarely used parameters are hidden. You can choose to make one or more of these parameters appear in the **Add Source** and **Source: ... General** pages of the Administration Tool so that you can change their default value. Consider changing values of hidden parameters when you encounter issues.

The following list describes the advanced hidden parameters available with Oracle Knowledge sources. The parameter type (integer, string...) appears between parentheses following the parameter name.

**DiscussionBoardCrawlerWebServiceUrl (String)**

The URL to the discussion board hidden crawler. Auto-filled with the starting address. The default and recommended value is


**ClientAPIWebServiceUrl (String)**

The URL to the client API web service. The default and recommended value is


**Locales (String)**

The specific languages of the content to index, separated by semi-colons i.e.: en_US; fr_FR. The default value is null, meaning that the connector indexes all locales.

**Example**: When you only want to index English documents, enter en_US.

**ItemTypesToIgnore (String)**

The type of Oracle Knowledge items to ignore while indexing, separated by semi-colons. The default value is null, meaning that the connector indexes all item types. Possible values are: Channel, ContentRecord, ContentRecordAttachment, DBForum, DBMessage, DPTopic, DiscussionBoard and Repository.

**ChannelReferenceKeys (String)**

The Oracle Knowledge channels to index, identified by their reference keys and separated by semi-colons. The
default value is null, meaning that the connector indexes all channels.

Use the following procedure only when you want to modify one or more of the above hidden source parameters.

To modify hidden Oracle Knowledge source parameters

1. Refer to "Adding an Explicit Connector Parameter" on page 450 to add one or more Oracle Knowledge hidden source parameters.

2. For a new Oracle Knowledge source, access the Add Source page of the Administration Tool to modify the value of the newly added advanced parameter:
   a. Select Index > Sources and Collections.
   b. Under Collections, select the collection in which you want to add the source.
   c. Under Sources, click Add.
   d. In the Add Source page, edit the newly added advanced parameter value.

3. For an existing Oracle Knowledge source, access the Source: ... General page of the Administration Tool to modify the value of the newly added advanced parameter:
   a. Select Index > Sources and Collections.
   b. Under Collections, select the collection containing the source you want to modify.
   c. Under Sources, click the existing Oracle Knowledge source in which you want to modify the newly added advanced parameter.
   d. In the Source: ... General page, edit the newly added advanced parameter value.

4. Rebuild your Oracle Knowledge source to apply the changes to the parameters.

9.34.7 Troubleshooting Oracle Knowledge Connector Issues

When configuring a security provider, the following error is displayed and the security provider is stated as Invalid:

An error occurred while initializing the Blade "Oracle Knowledge Security Provider" (ID #37): Unexpected exception in method 'InitBlade': System.IO.FileLoadException: Could not load file or assembly 'IQServiceClientCS. Version=8.1.1.32620. Culture=neutral. PublicKeyToken=44110d1682522' or one of its dependencies.

Possible cause

You did not have IQServiceClientCS.dll located on your machine hosting CES.

Possible solution

Add the client DLL in the CES 7 Bin folder:

1. Stop the CES service.

2. On the machine hosting Oracle Knowledge, copy the IQServiceClientCS.dll file located in the MSFT folder.
Example: C:\Oracle\Knowledge\IM\InfoManager\clientLibrary\MSFT\Release

3. On the machine hosting CES, paste the IQServiceClientCS.dll file in the Bin folder of CES.

Example: C:\Program Files\Coveo Enterprise Search 7\Bin

4. Restart the CES service.

When trying to index an Oracle Knowledge source, the following error is displayed and the operation is aborted:

Unable to establish a connection to the Service Client API at: http://[MyInQuiraServer]:8226/imws/WebObjects/imws.woa/ws/RequestProcessor/imws/WebObjects/imws.woa/ws/RequestProcessor, with user [Username]. Please ensure your configuration is correct -> Client found response content type of '', but expected 'text/xml'. The request failed with the error message: -- Your requested web service, namely "RequestProcessor/imws/WebObjects/imws.woa/ws/RequestProcessor", cannot be found in WOWebServiceRegistrar. --.

Possible cause

Your starting address ends with /imws/WebObjects/imws.woa/ws/RequestProcessor/ (see Configuring and Indexing an Oracle Knowledge Source).

Note: The /imws/WebObjects/imws.woa/ws/RequestProcessor/ part is automatically added by the connector to the end of your Oracle Knowledge server URL.

Possible solution

1. Remove /imws/WebObjects/imws.woa/ws/RequestProcessor/ at the end of the starting address parameter value (see Configuring and Indexing an Oracle Knowledge Source).

2. Try rebuilding the source by clicking Save and Start.

9.35 Oracle UCM Connector

The Coveo beta connector for Oracle UCM systems is introduced with Coveo Enterprise Search (CES) version 6.5. The connector allows to index the Content Server from one or more Oracle UCM servers, integrating that content into the CES unified index, and making it easily searchable by users. Oracle UCM Content Server is an automated system for sharing, managing, and distributing business information using a website as a common access point.

Note: Oracle rebranded the Oracle Universal Content Management (UCM) product to Oracle WebCenter Content Core Capabilities.

9.35.1 Features

The following details the features available in the Oracle UCM connector:

Content Indexing

The connector can retrieve and index exclusively the following default document types from Oracle UCM:
Any type of binary documents stored on the Content Server
Discussions associated to documents

Security
The permissions in CES use the same security model as Oracle UCM. The model is based on user access granted through Oracle UCM accounts, roles and security groups. Coveo users can search for any document to which they are granted access in Oracle UCM.

Limitations
- This connector does not support incremental refresh (but does include scheduled source refresh).
- For external authorization, only Microsoft Active Directory is supported.
- For external authorization using Active Directory, Credential Maps are not supported.
- Access Control List (ACL) security is not supported (see the Oracle topic Access Control List Security).
- Attachments are not supported.

What's Next?
Review the connector deployment process (see "Oracle UCM Connector Deployment Overview" on page 1395).

9.35.2 Oracle UCM Connector Deployment Overview
The following procedure outlines the steps needed to deploy the Oracle UCM connector. The steps indicate the order in which you must perform key CES configurations. When needed, the step refers to a detailed procedure.

1. Validate that your environment meets the requirements (see "Oracle UCM Connector Requirements" on page 1396).

2. On your Oracle UCM server:
   a. Allow access for the Coveo connector to the Oracle UCM server.
      You must configure the Oracle UCM server to grant direct access from the Coveo server (see "Configuring Oracle UCM to Allow Access from the Coveo Server" on page 1396).
   b. Create a dedicated crawling user on the Oracle UCM server.
      You must create a user with the same roles as the legacy sysadmin user that the crawler will use to access your Oracle UCM content (see "Creating an Oracle UCM Crawling Account" on page 1399).

3. On your Coveo server:
   a. Configure the user identity.
      The Coveo connector needs to know the credentials of the Oracle UCM crawling account that you created (see "Adding a User Identity" on page 420).
   b. Configure the security provider.
The Coveo connector needs to resolve mappings between users and groups from the Oracle UCM system and Microsoft Active Directory (see "Configuring an Oracle UCM Security Provider" on page 1403).

c. Configure and index the Oracle UCM source.

The Coveo connector needs to know details about the Oracle UCM system to be able to index its content (see "Configuring and Indexing an Oracle UCM Source" on page 1407).

d. Optionally, create and use a custom mapping file.

Create a custom mapping file only when you want to modify the default mapping of metadata retrieved from Oracle UCM documents (see "About the Oracle UCM Mapping File" on page 1412).

What’s Next?

Review the connector requirements (see "Oracle UCM Connector Requirements" on page 1396).

9.35.3 Oracle UCM Connector Requirements

Your environment must meet the following requirements to be able to use the Coveo connector for Oracle UCM systems:

- Coveo license for the Oracle UCM connector
  
  Your Coveo license must include support for the Oracle UCM connector to be able to use this connector.

- Oracle UCM version 10r3 or 11g
  
  The connector was developed and tested with both versions of Oracle UCM.

- Oracle UCM using either Local Authorization or External Authorization bound to Microsoft Active Directory
  
  While Oracle UCM does support External Authorization from any type of LDAP repository, the Oracle UCM connector only supports Microsoft Active Directory. When this is not the case, you can however manually map permissions (see "Configuring and Indexing an Oracle UCM Source" on page 1407).

What’s Next?

Configure the account used by CES to crawl the Oracle UCM content (see "Adding a User Identity" on page 420).

9.35.4 Configuring Oracle UCM to Allow Access from the Coveo Server

The Coveo connector requires direct access to the Oracle UCM Content Server to be able to crawl its content. You must ensure that Oracle UCM is allowing traffic from the IP address of the Coveo server.

To verify if the Oracle UCM configuration allows connection from the Coveo server

1. Log in to your Oracle UCM Content Server using an account with full access privileges.

2. In Oracle Content Server:
   a. In the navigation panel on the left, in the Administration section click Configuration for [Your_Oracle_UCM_instance].
   b. In the panel on the right, under System Configuration, click Server Configuration to expand the server
c. Verify that the Server IP Filter key name contains either *.*.*.* or the IP address of the Coveo Master server.

If it is not the case, use one of the following procedures to modify this parameter.

To configure Oracle UCM 10g to allow access from the Coveo server

1. Using an administrator account, connect to the Oracle UCM server.
2. Start the System Properties Oracle UCM utility:
   a. On the Windows Start menu, select All Programs > Oracle Content Server > [idc] > Utilities > System Properties, where [idc] is the name of your Oracle UCM instance.

   OR

   b. Double-click the [DomainHome]\bin\SystemProperties.exe file.
3. In the System Properties utility:
a. Select the **Server** tab.

b. In **IP Address Filter**, either add `*.*.*.*` to allow connections to the Oracle UCM server from any IP addresses or add the specific IP address of the Coveo Master server.

c. Click **OK**.

To configure Oracle UCM 11g to allow access from the Coveo server

1. Using an administrator account, connect to the Oracle UCM server.

2. Using a text editor:
   a. Open the `[DomainHome]\ucm\cs\config\config.cfg` file.

   **Example:** `C:\Oracle\Middleware\user_projects\domains\MySite\ucm\cs\config\config.cfg`

   b. Edit the `SocketHostAddressSecurityFilter` parameter to either include `*.*.*.*` to allow connections to the Oracle UCM server from any IP addresses or include the specific IP address of the Coveo Master server.
Example: SocketHostAddressSecurityFilter=*..*.*|0.0.0.0.0.0.0.1

| c. Save the file. |

What’s Next?

Create a dedicated crawling account (see “Creating an Oracle UCM Crawling Account” on page 1399).

9.35.5 Creating an Oracle UCM Crawling Account

The Coveo connector for Oracle UCM needs an account that has full access to your Oracle UCM server to be able to crawl and index your content.

Starting with Oracle UCM version 11g, the `sysadmin` account password is randomly defined by the installer and you no longer can change it using the `User Admin` applet. While the password could be changed directly in the database following a tedious procedure, using the `sysadmin` account as the crawling account is no longer a good option.

A better practice is simply to create an account for the exclusive use of the Coveo connector. This account must be a member of the same roles and have the same account permissions as the `sysadmin` account.

To create a dedicated Oracle UCM crawling account

1. Open the Oracle Content Server, by default using a URL in the http://[YourOracleUCMServer]:16200/cs form.

   **Note:** The Java JRE plugin must be installed in your browser.

2. In the navigation panel on the left, expand `Administration`, and then select `Admin Applets`.

3. In the main panel, click `User Admin`. 
4. In the User Admin dialog box, in the Users tab, select the sysadmin user, and then click Add Similar.
5. In the Add User dialog box:
   
a. In the Info tab, enter the mandatory Name and Password parameters, optionally filling the other parameters.
b. In the **Roles** tab, ensure that the **admin** and **sysmanager** roles are assigned.

c. In the **Accounts** tab, ensure that [all accounts] is assigned.
What's Next?

Create a user identity that holds the credentials of this Oracle UCM crawling account (see "Adding a User Identity" on page 420).

9.35.6 Configuring an Oracle UCM Security Provider

A security provider is required to properly set Oracle UCM Content Server documents permissions on Coveo search results.

Notes:

- As specified in the requirements (see "Oracle UCM Connector Requirements" on page 1396), only local Oracle UCM permissions and external authorization using Microsoft Active Directory are supported by the Oracle UCM connector. If this is not the case in your Oracle UCM environment, do not perform the following procedure. Your alternative is to set permissions manually on the source.

- You can get familiar with how Coveo components deal with permissions on documents both at indexing and query time.

To configure an Oracle UCM security provider

1. On the Coveo server, access the Administration Tool.
3. In the Security page, in the navigation panel on the left, click Security Providers.
4. In the Security Providers page, click Add to create a new security provider.
5. In the **Modify Security Provider** page:
a. Configure the following required parameters:

**Name**
Choose a significant name to identify the security provider.

**Security Provider Type**
In the drop-down list, select Oracle UCM (x64).

**User Identity**
Select the Oracle UCM user identity that you created previously.

**Active Directory Security Provider**
Select Active Directory or a custom Active Directory security provider that you created for a specific domain.

**UCM Server URL**
The address of the Oracle UCM Content Server web site. This should be the same address as the one specified when you configure the source for the connector (see "Configuring and Indexing an Oracle UCM Source" on page 1407). Enter the URL in the following format:

```
http://[ucm-host]/[idc]
```

where you replace `[ucm-host]` by the actual Oracle UCM server host name and `[idc]` by the name of the UCM instance to index.

b. Review the default value for the following optional parameters:

**UCM Server Port**
The listening port of the Oracle UCM Content Server. The default value is 4444.

**UCM Settings Life Time**
To improve performance, Oracle UCM role and account membership information is cached by the security provider. This parameter sets the time intervals between cache updates. The default value is 5 minutes.

c. When you use Oracle UCM external Active Directory permissions, include the following required parameters:

**Using Active Directory Security**
Select the check box to instruct this security provider to use UCM Active Directory permissions.

**Important:** For all LDAP URLs, you must enter the LDAP keywords (LDAP, OU, DC...) in uppercase.

**Users LDAP Search Root**
In the box, enter the Active Directory (AD) root location where Oracle UCM users are located. This parameter must be specified in LDAP format and must contain a valid domain naming context.
Example: LDAP://OU=UCM,DC=acme,DC=com"

Role LDAP Search Root

In the box, enter the Active Directory (AD) root location where Oracle UCM roles are located. This parameter must be specified in LDAP format.

While not required, you can specify a depth in the LDAP tree by adding brackets at the end of the LDAP string. When not specified, a depth of zero is assumed resulting in only AD groups within the specified AD being considered as Oracle UCM roles.

Example: LDAP://OU=UCM Roles,OU=UCM[1]

Accounts LDAP Search Root

The Active Directory (AD) root location where Oracle UCM accounts are located. This parameter must be specified in LDAP format. While not required, you can specify a depth in the LDAP tree by adding brackets at the end of the LDAP string. When not specified, a depth of zero is assumed resulting in only AD groups within the specified AD being considered as Oracle UCM accounts.

Example: LDAP://OU=UCM Accounts,OU=UCM[2]

d. When you use Oracle UCM external Active Directory permissions, you can also specify the following optional parameters:

Role LDAP Search Filters

In the box, enter the LDAP filter to apply to Active Directory (AD) groups when searching for Oracle UCM roles in the location specified by the Role LDAP Search Root parameter. No filter is defined by default.

Example: (role_filter=value*)

Role Name Prefix

In the box, enter the prefix used for Active Directory groups that represent Oracle UCM roles. If the prefix is found within the group name, only the right part is considered. No prefix is defined by default.

Example: With $RoleXYZ an Oracle UCM role can be $RoleXYZ.

Account LDAP Search Filters

In the box, enter the LDAP filter to apply to Active Directory groups when searching for Oracle UCM accounts in the location specified by the Account LDAP Search Root parameter. No filter is defined by default.

Example: (! (account_filter=value*))

Accounts Permission Delimiter

In the box, enter the delimiter used to optionally specify, in an Active Directory group name, the permission levels of the associated Oracle UCM account. If the delimiter is found within the group
name, only the left part is considered. The default value is "_".

**Example:** With _, an Oracle UCM account can be `AccountABC_rw`.

### Accounts Name Prefix

In the box, enter the prefix used for Active Directory groups that represent Oracle UCM accounts. If the prefix is found within the group name, only the right part is considered. The default value is @.

**Example:** With @, an Oracle UCM account can be `@AccountABC`.

### Default Network Account

In the box, enter the default network account.

### AD User Name

In the box, enter the username of the Windows user identity used to connect to Active Directory. When none is specified, the identity of the process running CES is used to connect to Active Directory. No username is defined by default.

### AD User Password

In the box, enter the password of the Windows user identity used to connect to Active Directory. When none is specified, the identity of the process running CES is used to connect to Active Directory. No password is defined by default.

1. In the **Parameters** section, in rare cases the Coveo Support could instruct you to click **Add Parameters** to specify other security provider parameter names and values that could help to troubleshoot security provider issues.

2. Leave the **Allow Complex Identities** option cleared as it does not apply to this type of security provider.

6. Click **Apply Changes**.

### What's Next?

Configure and index the Oracle UCM source (see "Configuring and Indexing an Oracle UCM Source" on page 1407).

### 9.35.7 Configuring and Indexing an Oracle UCM Source

A source defines a set of configuration parameters for a specific Oracle UCM server.

**Note:** In an environment with more than one Oracle UCM server, you need to define one source for each Oracle UCM server that you want to index.

To configure and index an Oracle UCM source

1. On the Coveo server, access the Administration Tool.

2. Select **Index > Sources and Collections**.

3. In the **Collections** section:
a. Select an existing collection in which you want to add the new source.

OR

b. Click Add to create a new collection.

4. In the Sources section, click Add.

The Add Source page that appears is organized in three sections.

5. In the General Settings section of the Add Source page:

![General Settings](image)

a. Enter the appropriate value for the following required parameters:

Name

A descriptive name of your choice for the connector source.

**Example:** Corporate Oracle UCM

Source Type

The connector used by this source. In this case, select Oracle UCM.

Addresses

The address of the Oracle UCM Content Server Website. This should be the same address that you entered for the ServerUrl parameter in the security provider (see "Configuring an Oracle UCM Security Provider" on page 1403). Enter the address in the form:
http://[ucm-host]/[idc]

where you replace [ucm-host] by the actual Oracle UCM server host name and [idc] by the name of the UCM instance to index.

Refresh Schedule

Time interval at which the index is automatically refreshed to keep the index content up-to-date. By default, the Every day option instructs CES to refresh the source everyday at 12 AM.

Because incremental refresh is not available for the Oracle UCM connector, ensure to select an appropriate source refresh schedule, as this is the only mechanism that ensures that the index content is kept up-to-date.

Notes:

- A refresh does not detect that an item needs to be re-indexed when only its metadata changes because the item itself has not been checked in.
- You can create new or modify existing source refresh schedules.

b. Review the value for the following parameters that often do not need to be modified:

Rating

Change this value only when you want to globally change the ranking associated with all items in this source relative to the rating of other sources.

**Example:** If this source was for a legacy system, you may want to set this parameter to Low, so that in the search interface, results from this source appear later in the list compared to those from other sources.

Document Types

If you created a custom document type set for this source, select it. Otherwise, select Default.

Active Languages

If you defined custom active language sets, ensure to select the most appropriate for this source.

Fields

If you defined custom field sets, ensure to select the most appropriate for this source.

6. In the **Specific Connector Parameters & Options** section of the **Add Source** page:
a. When you choose to customize how metadata is set on the CES documents using a mapping file, in the Mapping File box, enter the full path of your valid mapping file (see "About the Oracle UCM Mapping File" on page 1412). When this parameter is empty, the connector uses a generic mapping file.

Example: C:\CES7\UCM\Mapping.config

b. Review the default values for the following parameters:

**Number of Refresh Threads**

The number of simultaneous connections established with the Oracle UCM Content Server by the connector. Increasing this value may improve source refresh speed but puts more load on the Oracle UCM Content Server.

**Content Server Port**

The port used by the Oracle UCM Content Server.

*Note:* This value can be found by logging in the UCM Content Server and going to the Configuration > Server Configurations page. The default value for the Content Server port is 4444 and should not be mistaken with the Web Server port, which is usually 80 or 8080.

c. In the Parameters section, in rare cases the Coveo Support can instruct you to click Add Parameter to enter the name and value of hidden parameters that can help in troubleshooting issues.

d. In the Option section, the state of check boxes generally does not need to be changed:

**Index Subfolders**

Check to index all subfolders below the specified starting addresses.

**Index the document's metadata**

When selected, CES indexes all the document metadata, even metadata that are not associated with a field. The orphan metadata are added to the body of the document so that they can be searched using free text queries.
When cleared (default), only the values of system and custom fields that have the Free Text Queries attribute selected will be searchable without using a field query.

**Example:** A document has two metadata:

- `LastEditedBy` containing the value Hector Smith
- `Department` containing the value RH

In CES, the custom field `CorpDepartment` is bound to the metadata `Department` and its Free Text Queries attribute is selected.

When the Index the document's metadata option is cleared, searching for RH returns the document because a field is indexing this value. Searching for hector does not return the document because no field is indexing this value.

When the Index the document's metadata option is selected, searching for hector also returns the document because CES indexed orphan metadata.

**Document's addresses are case-sensitive**

Leave the check box cleared. This parameter needs to be checked only in rare cases for case sensitive systems in which distinct documents may have the same file name but with different casing.

**Generate a cached HTML version of indexed documents**

When you select this check box (recommended), at indexing time CES creates HTML versions of indexed documents and saves them in the unified index. In the search interfaces, users can then more rapidly review the content by clicking the Quick View link to open the HTML version of the item rather than opening the original document with the original application.

Consider clearing this check box only if you do not want to use Quick View links or to save resources when building the source.

**Open results with cached version**

Leave this check box cleared (recommended) so that in the search interfaces, the main search result link opens the original document with the original application. Consider selecting this check box only when you do not want users to be able to open the original document but only see the HTML version of the document as a Quick View. When this option is selected, you must also select the Generate a cached HTML version of indexed documents check box.

7. In the Security section of the Add Source page:
a. In the **Security Provider** drop-down list, select the Oracle UCM security provider that you created for this source (see "Configuring an Oracle UCM Security Provider" on page 1403).

b. In the **Authentication** drop-down list, select the Oracle UCM user identity that you created for this source.

c. Click **Save** to save the source configuration. Do not start indexing this source yet.

8. In the navigation panel on the left, click **General**.

9. In the **General** page, modify the **Title Selection Sequence** so that the **Use the filename** option is the first option at the top of the list.

10. In the navigation panel on the left, click **Permissions**.

11. In the **Permissions** page:

a. From the **Permissions** options:

   - Select **Use a Security Provider**, and then choose from the drop-down menu the security provider that you created for this source (see "Configuring an Oracle UCM Security Provider" on page 1403).

   OR

   i. Select the **Specify the security permissions to index** option when your Oracle UCM system uses External Authorization from a repository other than Microsoft Active Directory to manually specify the permissions that will be set on documents from this source.

   ii. In the **Allowed Users** and **Denied Users** boxes, respectively enter the allowed and denied users and groups for the source.

b. Click **Apply Changes**.

12. When you are ready to start indexing the Oracle UCM source, click **Start**.

13. In the navigation panel on the left, click **Status**, and then validate that the indexing proceeds without errors.

9.35.8 About the Oracle UCM Mapping File

The Oracle UCM mapping file is an XML formatted text file used by Coveo Enterprise Search (CES) to map metadata retrieved from an Oracle UCM document to CES fields.

The following mapping file code contains the default mappings used by the Oracle UCM connector.
In the mapping file, a Mapping entry associates a type of document indexed by CES with an Oracle UCM document type. These mappings are then used by the connector as directives to know which metadata from the UCM document must be assigned to which field (such as the Title) of the CES document. By editing this mapping file, it is possible to customize how the CES search results will be displayed to the end-user.

A custom mapping file is only required when you want to modify the default behavior of the Oracle UCM connector.

To create and use a custom mapping file

1. Using an administrator account, connect to the Coveo Master server.
2. Using a text editor:
   a. Use the content of the default mapping file as a starting point.
   b. While respecting the format of the mapping file, adapt the content of the mapping file to implement the desired custom mapping.
c. Save the file under the [Index_Path] folder using a subfolder and a filename of your choice.

Example: C:\CES7\UCM\Mapping.config

3. Access the Administration Tool, and then associate the mapping file to the desired Oracle UCM source:
   a. Select Index > Sources and Collections.
   b. In the Collections section, select the collection containing the source to which you want to add the mapping file.
   c. In the Sources section, select the source to which you want to add the mapping file.
   d. In the navigation panel on the left, click General.
   e. In the General page for the Oracle UCM source, for the Mapping File parameter, enter the full path to your custom mapping file.
   f. Click Apply Changes.

9.36 PTC Windchill Connector

CES 7.0.7256+ (December 2014)

Deprecated

The Coveo connector for PTC Windchill allows you to integrate the content of your PTC Windchill site together with associated permissions into your Coveo unified index, making this content easily and securely searchable by end-users.

The Coveo connector accesses the PTC Windchill product lifecycle management (PLM) content by indexing the PTC Windchill PDMLink data.

Note: As of March 2, 2017, the PTC Windchill connector is deprecated (see "What Does Deprecated Mean for a Coveo Connector?" on page 739).

9.36.1 Features

- Content indexing:
  - Site
  - Organizations (WTOrganization)
  - Products (PDMLinkProduct)
  - Libraries (WTLibrary)
  - Parts (WTPart)
    - Part usage
    - Alternate parts
Substitute parts
Reference documents
Described by documents
  - Documents (WTDocument)
  - CAD documents (EPMDocument)

Security model support
The connector and the security provider support the PTC Windchill security model by indexing permissions associated with each PTC Windchill entity, so that search results only contain documents the user performing the search has the rights to see.

The connector resolves the following security model entities:
  - Ad Hoc access control lists (ACL)
  - Policy access control lists (ACL)
  - Owner and All pseudo-roles (well-known), system and user-defined groups and dynamic roles

Language support
The connector retrieves the content of the PTC Windchill default locale language which can be English, Chinese (Traditional and Simplified), French, German, Italian, Japanese, Korean, Spanish, and Russian.

Incremental Refresh
Updated (added, edited, deleted) content items [Part, Document, EPM Document (CAD Part)] in a PTC Windchill site content holder are periodically re-indexed by the connector.

Notes:
- The delete events must be audited to be taken into account (see PTC Windchill Connector Deployment Overview).
- CES 7.0.7256 (December 2014) Deleted items require a full refresh to be taken into account.

9.36.2 Limitations
- Custom Soft Type attributes for parts, documents and CAD documents
  The connector can index the most common types (list)

Security limitations
The connector does not support the following security model aspect:
  - Security Labels (including Authorization agreements)
  - The connector and security provider do not take into account the following security aspects:
Profiles (only hide elements from the PTC Windchill interface without affecting the permissions)

Administrative lock (Do not affect the Read permission)

- Users performing the search have the rights to see the document if they have at least the Read or the Full control (All) permission. In the case of application data content items, the users must also have the Download permissions to see them.

**Connector Feature History**

<table>
<thead>
<tr>
<th>Coveo Platform version</th>
<th>Date</th>
<th>Features</th>
</tr>
</thead>
<tbody>
<tr>
<td>7.0.7338</td>
<td>January 2015</td>
<td>Improved incremental refresh support</td>
</tr>
<tr>
<td>7.0.7256</td>
<td>December 2014</td>
<td>Connector introduction</td>
</tr>
</tbody>
</table>

**What's Next?**

Review the steps for the deployment of the PTC Windchill connector (see "PTC Windchill Connector Deployment Overview" on page 1416).

**9.36.3 PTC Windchill Connector Deployment Overview**

The following procedure outlines the steps needed to deploy the PTC Windchill connector. The steps indicate the order in which you must perform key PTC Windchill and CES configurations. When needed, the step refers to a detailed procedure.

1. Validate that your environment meets the requirements (see "PTC Windchill Connector Requirements" on page 1418).

2. On your PTC Windchill server:
   a. Create a dedicated crawling account on the PTC Windchill server
      The connector needs an account that has read access to all the PTC Windchill content that you want to index. It is recommended to create a dedicated PTC Windchill account for this purpose.
   b. Copy PTC Windchill certificate files
      The Coveo connector needs to have access to a copy of the PTC Windchill client and server certificate files to be authorized to communicate with your PTC Windchill server (see "Copying the PTC Windchill Certificates to the Coveo Master Server" on page 1419).
   c. Install (or update) the Coveo plugin
      You must install the Coveo plugin on your PTC Windchill server to allow the connector to communicate with PTC Windchill (see "Installing or Updating the Coveo Plugin for PTC Windchill" on page 1420).
   d. When you want the incremental refresh to capture content items deletion, you must audit the delete events:
Note: CES 7.0.7338+ (January 2015) The incremental refresh supports deleted items.

i. With a text editor, open the XML PTC Windchill configAudit file located in the Windchill folder.

Example: C:\Program Files\Windchill\conf\auditing\configAudit.xml

ii. Ensure that the first line of the configAudit file is the following:

<EventConfiguration enabled="true">

meaning that the auditing is enabled within your PTC Windchill site.

iii. Under the <ConfigEntry class="" enabled="true"> node, add the following line to audit the delete events:

<KeyedEventEntry eventKey="/wt.events.summary.DeleteSummaryEvent/
 enabled="true" handler="wt.audit.configaudit.DefaultAuditEventRecorder"/>

iv. Under the <ConfigEntry class="" enabled="false"> node, remove the previous line.

Note: By default, delete events are not audited.

v. Save the file.

vi. Restart the method server to apply the new configuration.

3. On your Coveo server:

a. Configure a user identity

The Coveo connector needs to know the credentials of the PTC Windchill crawling account that you created (see "Adding a User Identity" on page 420).

b. Optionally, but recommended, create a PTC Windchill field set from the default XML field set file to be able to leverage PTC Windchill metadata for example to create more useful facets.

i. With a text editor, open the [CES_Path]\Bin\Coveo.CES.CustomCrawlers.Windchill.FieldSet.xml default XML PTC Windchill field set file and copy its content.

ii. Create a PTC Windchill field set by importing the XML file content.

c. Create a custom document type set

Note: Some Windchill file types such as CAD and CAM files are big in size. By default, those large files are downloaded, but not converted by the connector, causing a serious crawling delay. It is thus strongly recommended to index only the metadata of those documents to significantly improve the crawling performance.

i. Create a document type set.

The document type set is a copy of the Default one that you need to customize.
In the Document Type Sets page, click the document type set that you just created.

In the Document Type page, in the toolbar, click Add.

In the configuration page, only three parameters are relevant to fulfill:

i. In the first box, enter a descriptive Name for this document type.

Example: Windchill Files

ii. In the File Extensions box, enter the following list: .3dm; .acs; .asm; .CATPart; .CATProduct; .cgm; .cgr; .des; .dgm; .dwg; .ed; .edn; .edp; .edz; .emm; .emp; .evs; .exp; .frm; .g; .gbf; .hdr; .iam; .ibl; .icm; .idx; .igs; .imf; .ipt; .jt; .lay; .mdc; .mdf; .mem; .mfg; .model; .neu; .nwf; .obj; .pdt; .plt; .prt; .pts; .pvs; .pvt; .pvz; .rep; .rla; .sec; .session; .set; .shd; .sldasm; .sldprt; .step; .stl; .stp; .tsh; .tx1; .tx3; .tx4; .u3d; .vda; .wrl; .x_b; .x_n; .x_t; .xmt; .xmt_bin; .xmt_neu; .xmt_txt; .xpr

iii. Next to Indexing Failure Action, select the Index file information only radio button.

iv. Click Save.

d. Configure a security provider

The Coveo connector requires a PTC Windchill security provider to expand PTC Windchill groups and resolve mappings between users and groups from the PTC Windchill system and other systems like Microsoft Active Directory (see "Configuring a PTC Windchill Security Provider" on page 1422).

e. Configure and index a PTC Windchill source

The Coveo connector needs to know details about the PTC Windchill site to be able to index its content (see "Configuring and Indexing a PTC Windchill Source" on page 1425).

f. Optionally, modify hidden source parameters

If you encounter issues, review if modifying the default value of available hidden source parameters can resolve the issue you are facing (see "Modifying Hidden PTC Windchill Source Parameters" on page 1431).

g. In a Coveo search interface, validate that you and your end-users can see the allowed PTC Windchill documents in search results.

Note: You may need to manually update the CES security cache to see PTC Windchill documents in the search results.

What's Next?

Review the connector requirements (see "PTC Windchill Connector Requirements" on page 1418).

9.36.4 PTC Windchill Connector Requirements

Your environment must meet the following requirements to be able to use the Coveo connector for PTC Windchill.
Coveo license for the PTC Windchill connector

Your Coveo license must include support for the PTC Windchill connector to be able to use this connector.

**Supported PTC Windchill version**

The connector supports PTC Windchill PDMLink version 10.1 M010 and 10.1 M040 features.

**PTC Windchill security policy**

The connector plugin must be installed on a foreground method server that runs with the `userNameAuthSymmetricKeys` security policy and that has a keystore and a truststore (see "Copying the PTC Windchill Certificates to the Coveo Master Server" on page 1419 and "Installing or Updating the Coveo Plugin for PTC Windchill" on page 1420).

What’s Next?

Copy the PTC Windchill certificate files on the Coveo server (see "Copying the PTC Windchill Certificates to the Coveo Master Server" on page 1419).

9.36.5 Copying the PTC Windchill Certificates to the Coveo Master Server

The Coveo connector and security provider need to have access to a copy of the PTC Windchill client and server certificate files to be able to communicate with your PTC Windchill foreground method server. The Coveo connector will use the certificate file copies to authenticate itself with PTC Windchill to be able to connect to the Coveo plugin.

You must perform the following procedure only once after creating or updating your PTC Windchill certificates.

To copy the PTC Windchill foreground method server certificate to the Coveo Master server

1. If your PTC Windchill deployment contains more than one foreground method server, select one to be used by the Coveo connector.

2. Using an administrator account, connect to the PTC Windchill foreground method server.

3. Open a Windchill shell.

   **Example:** When PTC Windchill runs on a Windows Server, from the Start menu, select Windchill Shell.

4. When the keystore and truststore do not yet exist on your PTC Windchill foreground method server (with the `userNameAuthSymmetricKeys` default security policy), create them as follows:

   a. In the Windchill shell, run the following command:

   ```
   ant -f jws-stores.xml
   ```
b. Answer to the prompts of the script using the default or appropriate values (based on the security.properties file content).

Note: Refer to the Understanding the Security Requirements topic in the Windchill Help Center on your PTC Windchill server for more information.

5. Copy the PTC Windchill certificate files to the Coveo Master server:
   a. From the PTC Windchill foreground method server, copy the following files:
      ```
      %WT_HOME%\prog_examples\jws\stores\client.cer
      %WT_HOME%\prog_examples\jws\stores\server.cer
      ```
      where %WT_HOME% is the PTC Windchill home folder, such as C:\ptc\Windchill_10.x\Windchill.
   b. Using an administrator account, connect to the Coveo Master server.
   c. Paste the certificate files on the Coveo Master server in a [Index_Path] subfolder such as
      \CertStore\PTC_Windchill\.
      
      Example: On the Coveo Master server, copy the certificate files to the D:\CES7\CertStore\PTC_Windchill folder.

What's Next?

Install or update the Coveo plugin on your PTC Windchill server (see "Installing or Updating the Coveo Plugin for PTC Windchill" on page 1420).

9.36.6 Installing or Updating the Coveo Plugin for PTC Windchill

The Coveo connector for PTC Windchill needs a plugin to be able to access the PTC Windchill API. You must install the Coveo plugin on the PTC Windchill foreground method server.

When you upgrade CES, if the included PTC Windchill plugin is updated, you must also use this procedure update it on your PTC Windchill foreground method server.

To install or update the Coveo plugin on the PTC Windchill foreground method server

1. If your PTC Windchill deployment contains more than one foreground method server, select one to be used by the Coveo connector from which you also copy the certificates (see "Copying the PTC Windchill Certificates to the Coveo Master Server" on page 1419).
2. Using an administrator account, connect to your Windchill Server foreground method server.
3. Open a Windchill shell.

www.coveo.com
Example: When PTC Windchill runs on a Windows Server, from the Start menu, select Windchill Shell.

4. When the Coveo plugin is already installed on your PTC Windchill foreground method server and you are updating the plugin, you must first:

**Important:** Do not perform this step if you are installing the Coveo plugin for the first time.

a. Uninstall the previous plugin version by running the following command in a Windchill shell:

```
ant -f %WT_HOME%/bin/adminTools/WebServices/build.xml -Dservlet.name=CoveoWindchillWebService undeployService
```

b. It is recommended to rename the previous version of the plugin file as a backup.

**Example:** Rename the plugin .jar file to %WT_HOME%/codebase/WEB-INF/lib/CoveoWindchillWebService.jar.OLD

5. Copy the Coveo plugin file from the Coveo Master server to the PTC Windchill foreground method server:

a. On the Coveo Master server, copy the PTC Windchill plugin file:

[CES_Path]/bin/CoveoWindchillWebService.jar

b. Paste the plugin file on the PTC Windchill foreground method server in the following folder:

%WT_HOME%/codebase/WEB-INF/lib/

6. On the PTC Windchill foreground method server, install the plugin by running the following command in a Windchill shell:

```
ant -f %WT_HOME%/bin/adminTools/WebServices/build.xml -Dservlet.name=CoveoWindchillWebService -Dwebservice.class=coveo.WindchillWebService -Dsecurity.policy=userNameAuthSymmetricKeys deployFromJava
```

7. In a browser, you can validate that the installation completed successfully by ensuring the service WSDL is available with the following URL:

```
http://[WindchillWebServer]/Windchill/servlet/CoveoWindchillWebService?wsdl
```

The plugin Web Services Description Language (WSDL) similar to the following capture should appear.
What's Next?

Configure a CES user identity for the PTC Windchill crawling account credentials (see “Adding a User Identity” on page 420).

9.36.7 Configuring a PTC Windchill Security Provider

The PTC Windchill connector needs a security provider to manage the user permissions on PTC Windchill entities. The PTC Windchill security provider performs tasks such as expanding groups to users and mapping PTC Windchill users to emails or to Active Directory users. The connector creates and sets several virtual groups on indexed documents to support the access policies defined in PTC Windchill.

**Note**: You can get familiar with how Coveo components deal with permissions on documents both at indexing and query time.

To Configure a PTC Windchill security provider

1. On the Coveo server, access the Administration Tool.
2. Select **Configuration > Security**.
3. In the **Security** page, in the navigation panel on the left, click **Security Providers**.
4. In the **Security Providers** page, click **Add** to create a new security provider.
5. In the **Modify Security Provider** page:
a. In the **Name** box, enter a name to identify this security provider.

   **Example:** PTC Windchill Security Provider

b. In the **Security Provider Type** drop-down list, select **Windchill**.

c. In the **User Identity** section:
   
i. In the drop-down list, select the user identity that you created previously with the PTC Windchill crawling account credentials (see PTC Windchill Connector Deployment Overview).
   
   ii. When needed, click **Add**, **Edit**, or **Manage user identities** respectively to create, modify, or manage user identities.

d. In the **Coveo plug-in Web Service Url** box, enter the URL in the following format:

   \[http://[myWindchillServer]/Windchill/servlet/CoveoWindchillWebService\]

   where you replace `[myWindchillServer]` with the name of your PTC Windchill server.

e. In the **Client Certificate Path** and **Server Certificate Path** boxes, enter the path and file name where you copied these files on the Coveo Master server (see "Copying the PTC Windchill Certificates to the Coveo Master Server" on page 1419).
Example: When the files were copied with their original names in the D:\CES7\CertStore\PTC_Windchill\ folder, respectively enter:

- D:\CES7\CertStore\PTC_Windchill\client.cer
- D:\CES7\CertStore\PTC_Windchill\server.cer

f. In the Cache Entry Absolute Expiration box, leave the 30 seconds default value unless instructed to change it by Coveo Support.

This parameter indicates at what interval the security provider cache is reset. The use of this cache minimizes calls made to the plugin to retrieve policies. A value of 0 means no cache is used.

g. Select the Viewing Application Data Only Requires Download Permission check box only when you want the security provider to allow access to ApplicationData type documents (Windchill local files) when a user has only the Download permission, rather than by default, when the user has the Read+Download permissions.

Note: When you select this parameter, you must also add the ViewingApplicationDataOnlyRequiresDownloadPermission source parameter and set it to true (see Modifying Hidden PTC Windchill Source Parameters).

h. In the Security Provider section, optionally select another security provider to allow the PTC Windchill security provider to map PTC Windchill accounts to another user type with which people are authenticated when they perform a search:

- Select None when you do not want to map PTC Windchill users to another user type.

The security provider creates user members with the LDAP distinguished name (DN) retrieved from PTC Windchill.

- When the Windchill LDAP is synchronized with an Active Directory, select the out-of-the-box Active Directory security provider to map PTC Windchill users to AD users.

The PTC Windchill security provider maps users to Active Directory by extracting the UID of the LDAP distinguished name (DN) provided by Windchill.

Example: When a PTC Windchill user distinguished name (DN) is uid=jbaker,ou=people,cn=administrativeldap,cn=windchill_10.1,o=ptc, the security provider outputs a SID declarator with the name jbaker by extracting the UID of this DN.

Note: When a user exists in PTC Windchill, but does not exist in the Active Directory, a SID declarator is still created, but the Active Directory security provider will throw a SecurityInvalidUserGroupException because no mapping exists between this account and Active Directory.

- When the email property is defined for all users in PTC Windchill and your users authenticated with this email when they perform a search, you can click Add to create, and then select an Email security provider (see "Configuring an Email Security Provider" on page 65).
Note: When none of the above security provider types fulfill your needs, it may be possible to use a custom security provider like the REGEX Transform Member Name to bridge the gap between PTC Windchill accounts and another type of users (see "Configuring a REGEX Transformation Security Provider" on page 67).

i. (Optional) In the Parameters section, click Add Parameter and then use the following hidden parameter when you want to map your PTC Windchill usernames to their Windows usernames:

**ActiveDirectoryDomainNameForMappings ** CES 7.0.7433+ (February 2015)

Enter the Active Directory domain name used to map users in the Active Directory security provider. The default value is null. Consider changing the value when the Active Directory domain on which CES runs is not the desired domain.

**Example:** When the ActiveDirectoryDomainNameForMappings parameter value is MyCompany and you expand the PTC Windchill user John, the security provider will expand this user to the AD user MyCompany\John.

**Note:** This parameter is only used if you selected Active Directory in the Security Provider section (see step h).

j. Leave the Allow Complex Identities option cleared as it does not apply to this type of security provider.

k. Click Apply Changes.

What’s Next?

Configure and index your PTC Windchill source (see "Configuring and Indexing a PTC Windchill Source" on page 1425).

9.36.8 Configuring and Indexing a PTC Windchill Source

A source defines a set of configuration parameters for indexing the content of a specific PTC Windchill site.

To configure and index a PTC Windchill source

1. On the Coveo server, access the Administration Tool.

2. Select Index > Sources and Collections.

3. In the Collections section:

   a. Select an existing collection in which you want to add the new source.

   OR

   b. Click Add to create a new collection.

4. In the Sources section, click Add.

   The Add Source page that appears is organized in three sections.

5. In the General Settings section of the Add Source page:
a. Enter the appropriate value for the following required parameters:

**Name**

A descriptive name of your choice for the connector source.

Example: PTC Windchill Site

**Source Type**

The connector used by this source. In this case, select Windchill.

**Addresses**

The address of the PTC Windchill site in the form:

http://[PTCWindchillServer]/Windchill

where you replace [PTCWindchillServer] by your actual PTC Windchill server host name.

**Fields**

If you defined a PTC Windchill field set, select it (see PTC Windchill Connector Deployment Overview).

**Refresh Schedule**

Time interval at which the index is automatically refreshed to keep the index content up-to-date. By default, the Every day option instructs CES to refresh the source everyday at 12 AM. Because the incremental refresh takes care of maintaining the source up-to-date, you can select a longer interval such as Every Sunday.
Note: You can create a new or modify an existing source refresh schedule.

b. Review the value for the following parameters that often do not need to be modified:

Rating
Change this value only when you want to globally change the ranking associated with all items in this source relative to the rating of other sources.

Example: If this source is for a legacy PLM, you may want to set this parameter to **Low**, so that in the search interface, results from this source appear later in the list compared to those from other sources.

Document Types
Select the custom document type set that you created for this source (see PTC Windchill Connector Deployment Overview). Otherwise, leave **Default**.

Active Languages
If you defined custom active language sets, ensure to select the most appropriate for this source.

6. In the **Specific Connector Parameters & Options** section of the **Add Source** page:

   a. Enter the appropriate value for the following required parameters:

   Application URL
Enter the URL of the PTC Windchill application used to open search results.

   Example: `http://MyWindchillServer/Windchill/app/`
Web Service URL
Enter the URL to the Coveo plug-in web service.

Example: http://MyWindchillServer/Windchill/servlet/CoveoWindchillWebService

Server Certificate Path
Enter the path of the server X.509 certificate used to connect to the Coveo plug-in web service.

Example: E:\CES70\CertStore\PTC_Windchill\server.cer

b. In the Number of Refresh Threads box, consider changing the number of simultaneous connections established with the PTC Windchill site by the connector. The default value is 2. Increasing this value may improve source refresh speed but puts more load on the PTC Windchill server.

c. In the Mapping File box, leave the default mapping file name (Coveo.CES.CustomCrawlers.Windchill.MappingFile.xml) unless you created a custom mapping file, in which case, enter the full path of your valid mapping file.

d. Click Add Parameter when you want to show and change the value of hidden source parameters (see "Modifying Hidden PTC Windchill Source Parameters" on page 1431).
Notes:

- In rare cases, Coveo Support can instruct you to click Add Parameter to enter the name and value of other hidden parameters that can help in troubleshooting issues (see "Modifying Hidden PTC Windchill Source Parameters" on page 1431).

- **CES 7.0.7256—(December 2014)** The following required parameters must be added manually:

<table>
<thead>
<tr>
<th>Parameter name</th>
<th>Parameter value example</th>
</tr>
</thead>
<tbody>
<tr>
<td>ApplicationUrl</td>
<td><a href="http://MyWindchillServer/Windchill/app/">http://MyWindchillServer/Windchill/app/</a></td>
</tr>
<tr>
<td>ClientCertificatePath</td>
<td>E:\CES70\CertStore\PTC_Windchill\client.cer</td>
</tr>
<tr>
<td>ServerCertificatePath</td>
<td>E:\CES70\CertStore\PTC_Windchill\server.cer</td>
</tr>
<tr>
<td>WebServiceUrl</td>
<td><a href="http://MyWindchillServer/Windchill/servlet/CoveoWindchillWebService">http://MyWindchillServer/Windchill/servlet/CoveoWindchillWebService</a></td>
</tr>
</tbody>
</table>

Specific Connector Parameters & Options

- **Number of Refresh Threads**: 2
- **Mapping File**: Coveo/Custom/Indexes/Windchill/Map

Parameters

<table>
<thead>
<tr>
<th>Name</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>ApplicationUrl</td>
<td><a href="http://MyWindchillServer/Windchill/app/">http://MyWindchillServer/Windchill/app/</a></td>
</tr>
<tr>
<td>ClientCertificatePath</td>
<td>E:\CES70\CertStore\PTC_Windchill\client.cer</td>
</tr>
<tr>
<td>ServerCertificatePath</td>
<td>E:\CES70\CertStore\PTC_Windchill\server.cer</td>
</tr>
<tr>
<td>WebServiceUrl</td>
<td><a href="http://MyWindchillServer/Windchill/servlet/CoveoWindchillWebService">http://MyWindchillServer/Windchill/servlet/CoveoWindchillWebService</a></td>
</tr>
</tbody>
</table>

- **Option**: Check Subfolders

  - **Option**: Check Index the document’s metadata

    When selected, CES indexes all the document metadata, even metadata that are not associated with a field. The orphan metadata are added to the body of the document so that they can be searched using free text queries.

    When cleared (default), only the values of system and custom fields that have the Free Text Queries attribute selected will be searchable without using a field query.
Example: A document has two metadata:
- LastEditedBy containing the value Hector Smith
- Department containing the value RH

In CES, the custom field CorpDepartment is bound to the metadata Department and its Free Text Queries attribute is selected.

When the Index the document's metadata option is cleared, searching for RH returns the document because a field is indexing this value. Searching for hector does not return the document because no field is indexing this value.

When the Index the document's metadata option is selected, searching for hector also returns the document because CES indexed orphan metadata.

Document's addresses are case-sensitive

Leave the check box cleared. This parameter needs to be checked only in rare cases for case sensitive systems in which distinct documents may have the same file name but with different casing.

Generate a cached HTML version of indexed documents

When you select this check box (recommended), at indexing time CES creates HTML versions of indexed documents and saves them in the unified index. In the search interfaces, users can then more rapidly review the content by clicking the Quick View link to open the HTML version of the item rather than opening the original document with the original application.

Consider clearing this check box only if you do not want to use Quick View links or to save resources when building the source.

Open results with cached version

Leave this check box cleared (recommended) so that in the search interfaces, the main search result link opens the original document with the original application. Consider selecting this check box only when you do not want users to be able to open the original document but only see the HTML version of the document as a Quick View. When this option is selected, you must also select the Generate a cached HTML version of indexed documents check box.

7. In the Security section of the Add Source page:
a. In the **Security Provider** drop-down list, select the PTC Windchill security provider that you created for this source (see "Configuring a PTC Windchill Security Provider" on page 1422).

b. In the **Authentication** drop-down list, select the PTC Windchill user identity that you created for this source (see PTC Windchill Connector Deployment Overview).

c. Click **Save and Start** to save the source configuration and build the source.

8. Validate that the indexing proceeds without errors:

   a. In the navigation panel on the left, click **Status** to monitor the indexing progress.

   b. On the Coveo Master server, open the CES Console to review indexing logs.

### 9.36.8.1 Modifying Hidden PTC Windchill Source Parameters

The **Add Source** and **Source: ... General** pages of the Administration Tool present the parameters with which you can configure the connector for most PTC Windchill sites. More advanced and more rarely used parameters are hidden. You can choose to make one or more of these parameters appear in the **Add Source** and **Source: ... General** pages of the Administration Tool so that you can change their default value.

The following list describes the available advanced hidden parameters for PTC Windchill sources. The parameter type (integer, string…) appears between parentheses following the parameter name.

**BatchSize (Integer)**

The number of items to retrieve with each call to the web service. The default value is 100.

**UseVirtualGroupsPermissionModel (Boolean)**

Whether to use the permission model with virtual groups expanded by the security provider. The default value is `true`.

By default, each permission set on documents to support policy access control lists (ACL) contains virtual groups as members. These virtual groups are expanded by the security provider to fill allowed and denied members and are maintained in the security cache. The connector can directly expand members when this parameter is set to `false` so that permissions are stored directly in the index.

It can be useful to set this parameter to `false` if the permission model gets too complex and may not scale. The disadvantage is that you must rebuild the source to catch permission changes rather than simply update the security cache.

**ViewingApplicationDataOnlyRequiresDownloadPermission (Boolean)**

Whether the Download permission is sufficient to access Application Data type documents, rather than the default Read+Download permissions. The default value is `false`.

The Coveo security provider cannot currently resolve the combined Read+Download permissions so by default, users will never see Application Data type documents in search results. Set this parameter to `true` when you want to allow users having the Download permission (with or without the read permission) for documents of this type to see them in search results.

When you change this parameter you must also select the **Viewing Application Data Only Requires Download Permission** security provider option (see Configuring a PTC Windchill Security Provider).
WebAppUrlFragment (String)

The web app URL fragment of the PTC Windchill application used to open search results. The default value is /app/#ptc1. Change this value only if you use a web app other than the default one.

OrganizationIdentifiers (String) CES 7.0.7711+ (June 2015)

The list of organization container IDs (separated by a semicolon) of the organization you wish to index.

Note: To find the organization ID, as a Windchill Admin, access the Details page of an organization and looks at the URL of the page. In the following capture, the container ID is 12345.

To modify hidden PTC Windchill source parameters

1. Refer to "Adding an Explicit Connector Parameter" on page 450 to add one or more PTC Windchill hidden source parameters.

2. For a new PTC Windchill source, access the Add Source page of the Administration Tool to modify the value of the newly added advanced parameter:

   a. Select Index > Sources and Collections.

   b. Under Collections, select the collection in which you want to add the source.

   c. Under Sources, click Add.

   d. In the Add Source page, edit the newly added advanced parameter value.

3. For an existing PTC Windchill source, access the Source: ... General page of the Administration Tool to modify the value of the newly added advanced parameter:

   a. Select Index > Sources and Collections.

   b. Under Collections, select the collection containing the source you want to modify.

   c. Under Sources, click the existing PTC Windchill source in which you want to modify the newly added advanced parameter.

   d. In the Source: ... General page, edit the newly added advanced parameter value.
9.37 RSS Connector

**CES 7.0.6942+ (August 2014)**

RSS (Rich Site Summary) is a format for delivering regularly changing web content such as blog entries and news headlines. An RSS document called a *feed or channel* includes full or summarized text together with metadata, like publishing date and author's name.

The RSS connector allows you to bring RSS feed content into your Coveo unified index to make it easily searchable by end-users.

### 9.37.1 Connector Features Summary

<table>
<thead>
<tr>
<th>Features</th>
<th>Supported</th>
<th>Additional information</th>
</tr>
</thead>
<tbody>
<tr>
<td>RSS feeds version</td>
<td>RSS 1.0, RSS 2.0, and Atom 1.0</td>
<td></td>
</tr>
<tr>
<td>Searchable content types</td>
<td>✓</td>
<td>RSS feeds (or channels) and RSS items</td>
</tr>
<tr>
<td>Content update</td>
<td>Incremental refresh</td>
<td>✓</td>
</tr>
<tr>
<td></td>
<td>Full refresh</td>
<td>✓</td>
</tr>
<tr>
<td></td>
<td>Rebuild</td>
<td>✓</td>
</tr>
<tr>
<td>Document-level security</td>
<td>✗</td>
<td>Permissions must be manually defined on the source [more]</td>
</tr>
</tbody>
</table>

### 9.37.2 Features

The features of the RSS connector are:

**Content indexing**

The connector can retrieve and index exclusively the following RSS types of items:

- RSS feeds (or channels)
- RSS items

**Supported standards**

- RSS 2.0/1.0
- Atom 1.0
- OpenSearch extension
When the indexed RSS feed supports OpenSearch, on a full refresh or a rebuild the connector automatically can get all items including the old ones that are no longer part of the latest feed document.

**Incremental refresh**

The connector supports incremental refresh allowing to maintain the source up-to-date by indexing new, changed, or deleted RSS feed items at regular short intervals.

**Note:** The last modified date attribute must be set for each RSS feed item. Otherwise, the connector sets the default min value and you need to perform a source full refresh or rebuild to update changes on items.

Depending on the RSS feed format, the following property must be defined for each item:

- **Atom 1.0:** `<updated>`
- **RSS 2.0:** `<a10:updated>`

**Feature history**

<table>
<thead>
<tr>
<th>CES version</th>
<th>Monthly release</th>
<th>Features</th>
</tr>
</thead>
<tbody>
<tr>
<td>7.0.8225</td>
<td>March 2016</td>
<td>Connector provides default field set</td>
</tr>
<tr>
<td>7.0.6942</td>
<td>August 2014</td>
<td>Connector introduction</td>
</tr>
</tbody>
</table>

9.37.3 Configuring and Indexing an RSS Source

A source defines a set of configuration parameters for one or more RSS feeds.

To configure and index a source with the RSS connector

1. Ensure that your environment meets the RSS source requirements:
   - **CES 7.0.6942+ (August 2014)**
     - RSS connector included in your Coveo license (see "What Information Is Displayed in the License Page?" on page 525).

2. On the Coveo server, access the Administration Tool.

3. **CES 7.0.8225+ (March 2016)** Create an RSS field set to take advantage of the available RSS metadata.
   a. Import the default RSS field set file `{CES_Path}`\Bin\Coveo.CES.CustomerCrawlers.RSSCrawler.FieldSet.xml to create fields for all the metadata available by default from RSS documents.
   b. When you created custom metadata for your RSS documents, add corresponding fields to the field set.

4. Select **Index > Sources and Collections.**

5. In the **Collections** section:
a. Select an existing collection in which you want to add the new source.

OR

b. Click Add to create a new collection.

6. In the Sources section, click Add.

7. In the General Settings section of the Add Source page:

   a. Enter the appropriate value for the following required parameters:

   **Name**
   
   Enter a descriptive name of your choice for the connector source.

   **Example:** CNN Technology RSS Feed

   **Source Type**
   
   The connector used by this source. In this case, select RSS.

   **Addresses**
   
   Enter the URL of the RSS feed to index by simply copying and pasting the corresponding RSS feed link in either the file:// or http:// form.

   **Examples:** To index the Stack Overflow feed, the URL is:

   http://stackoverflow.com/feeds
You can enter more than one RSS feed address on separate lines, but you must ensure that all source parameters apply to all RSS feeds. Otherwise, create other sources for other feeds.

**Refresh Schedule**

Unless your RSS feeds supports OpenSearch (see "OpenSearch extension" on page 1433), select **(none)** when you want to keep in your source previously indexed old RSS items that are no longer available from the RSS feed. A full refresh, like a rebuild, deletes from the source the old items that are no longer available from the feed.

Select an interval like **every day** when you want to only make the latest feeds searchable.

**Notes:** Configure an incremental refresh schedule on your source to continuously maintain the source up-to-date.

b. Review the value for the following parameters that often do not need to be modified:

**Rating**

Change this value only when you want to globally change the rating associated with all items in this source relative to the rating to other sources.

**Example:** If this source was for an important RSS feed, you may want to set this parameter to **High**, so that in the search interface, results from this source appear earlier in the search result list compared to those from other sources.

**Document Types**

If you defined custom document type sets, ensure to select the most appropriate for this source.

**Active Languages**

If you defined custom language sets, ensure to select the most appropriate for this source.

**Fields**

_Editable CE 7.0.8225+ (March 2016)_ Select the field set that you created earlier (see **RSS field set**).

If you created a custom RSS field set for this source, select it. Otherwise, leave the **Default Scheme**.

**Note:** _CES 7.0.8047– (December 2015)_ If you created a custom RSS field set for this source, select it. Otherwise, leave the **Default Scheme**.

8. In the **Specific Connector Parameters & Options** section of the **Add Source** page:
Specific Connector Parameters & Options

Mapping File

Index RSS feed URL

Parameters

Option

a. Review if you need to change the default values for the following parameters:

**Number of Refresh Threads**

Determines the number of simultaneous downloads handled by the connector for this source. The default value is 2.

**Mapping File**

The path to the mapping file. Leave the default value to use the default mapping file that comes with the connector (Coveo.CES.CustomCrawlers.RSSCrawler.MappingFile.xml). If you create a custom mapping file, enter the full path to your custom mapping file. Contact Coveo Support for assistance if you need to customize the mapping file.

**Index RSS feed URL CES 7.0.9167+ (December 2017)**

Whether to index the URL of the RSS feed. By default, the RSS feed URL is not indexed.

b. In the **Option** section, review the default value of the following check boxes:

**Index Subfolders**

Check to index all subfolders below the specified RSS server address. Selected by default.

**Index the document’s metadata**

When selected, CES indexes all the document metadata, even metadata that are not associated with a field. The orphan metadata are added to the body of the document so that they can be searched using free text queries.

When cleared (default), only the values of system and custom fields that have the **Free Text Queries** attribute selected will be searchable without using a field query.
Example: A document has two metadata:
- LastEditedBy containing the value Hector Smith
- Department containing the value RH

In CES, the custom field CorpDepartment is bound to the metadata Department and its Free Text Queries attribute is selected.

When the Index the document's metadata option is cleared, searching for RH returns the document because a field is indexing this value. Searching for hector does not return the document because no field is indexing this value.

When the Index the document's metadata option is selected, searching for hector also returns the document because CES indexed orphan metadata.

Generate a cached HTML version of indexed documents

When you select this check box (recommended), at indexing time, CES creates HTML versions of indexed documents. In the search interfaces, users can then more rapidly review the content by clicking the Quick View link rather than opening the original document with the original application. Consider clearing this check box only if you do not want to use Quick View links or to save resources when building the source.

Open results with cached version

Leave this check box cleared (recommended) so that in the search interfaces, the main search result link opens the original document with the original application. Consider selecting this check box only when you do not want users to be able to open the original document but only see the HTML version of the document as a Quick View. In this case, you must also select Generate a cached HTML version of indexed documents.

c. Click Save to save the source configuration.

9. Because RSS feeds are not secured, the RSS connector does not index permissions and you must change the default Permissions option to set the permissions globally on the source:

Note: You get the following error message in the CES Console when the Index security permissions option is selected by default:

Permissions indexing is not provided by the RSS crawler. You must manually configure the permissions for the source '[Source_Name]'.

a. In the navigation panel on the left, select Permissions.

b. In the Permissions page:
i. Select the **Specifies the security permissions to index** option.

ii. Optionally, in the **Allowed Users** list, add or remove users or groups to precisely specify who has access to the content from this source.

   By default, the Active Directory **everyone** group specifies that any Active Directory user can see all the content from this source.

iii. Optionally, in the **Denied Users** list, add users or groups to specify who has not access to the content from this source.

iv. Click **Apply Changes**.

10. On the toolbar, click **Start/Rebuild** to start indexing your source.

11. Validate that the source building process is executed without errors:

   - In the navigation panel on the left, click **Status**, and then validate that the indexing proceeds without errors.

   OR

   - Open the CES Console to monitor the source building activities.

What's Next?

Set an incremental refresh schedule for your source to maintain your source up-to-date with the RSS feed.
9.38 Salesforce Connector

**CES 7.0.5785+ (August 2013)**

The on-premises Salesforce connector is part of the Coveo for Salesforce license and is therefore available only with Coveo for Salesforce (see Coveo for Salesforce).

The Coveo Salesforce connector allows you to crawl Salesforce content and bring it into the unified index, making it easily searchable by end-users.

**Important:** Salesforce no longer supports TLS 1.0 which is used by the Coveo connector for Salesforce in CES 7.0.8047– (December 2015) to retrieve Salesforce content and content updates. In the CES Console, you will get errors such as:

Salesforce2 Error: Could not establish secure channel for SSL/TLS with authority 'domain.salesforce.com'

You must thus upgrade CES to CES 7.0.8225+ (March 2016). Otherwise, you will no longer be able to update your Salesforce source content.

9.38.1 Advantages Relative to the Legacy Connector

This second generation Salesforce connector offers the following advantages over the Salesforce Legacy connector:

- Indexing of Salesforce permissions rather than applying the same permission on all source items (see "Indexed Salesforce Security" on page 1441)
- Improved performance and reduced API calls
- Indexing of Knowledge Base articles and CRM content files
- Takes advantage of recent Salesforce API versions

9.38.2 Connector Features Summary

<table>
<thead>
<tr>
<th>Features</th>
<th>Supported</th>
<th>Additional information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Salesforce versions</td>
<td>API 30 to API 34</td>
<td>Service Cloud standard/custom objects and fields, Chatter feed items and files, multilingual Knowledge base articles and attachments, and CRM content (binary files such as PDF).</td>
</tr>
<tr>
<td>Searchable content types</td>
<td>✅</td>
<td></td>
</tr>
</tbody>
</table>
### 9.38.3 Features

**Indexed Salesforce Content**

The connector can index the following Salesforce content:

- Service Cloud standard/custom objects and fields
- Multilingual Knowledge base articles
- Chatter feed items and files [more]
- CRM Content (binary files such as PDF)
- Sharing permissions
- Sandbox and production environments
- Inactive users
- User visibility

**Note:** The Salesforce connector does not support to rebuild only one KB or Chatter document or one whole object as it appears to be possible from the index browser.

**Indexed Salesforce Security**

The connector can index the permissions of each Salesforce item allowing the index to only return Salesforce search results that the user performing the query has the permissions to see.

The Coveo index replicates the Salesforce security model for:

<table>
<thead>
<tr>
<th>Features</th>
<th>Supported</th>
<th>Additional information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Content update</td>
<td></td>
<td><strong>Full refresh or rebuild needed to retrieve:</strong>&lt;br&gt;  - Attached and detached KB articles from cases&lt;br&gt;  - Deleted KB articles.&lt;br&gt;  - Not replicable deleted objects such as deleted ContentVersion (CRM Content and Chatter files) attachments and other items.&lt;br&gt;  - Changes that occurred more than 30 days ago since the last refresh (a scheduled refresh triggers a rescan).&lt;br&gt;  - Permission changes for a profile, permission set, object sharing, or object security level.</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Full refresh</strong>&lt;br&gt; <strong>Rebuild</strong></td>
</tr>
<tr>
<td>Document-level</td>
<td></td>
<td><strong>Does not support the following security aspects:</strong> Apex managed sharing, IP based permissions, field level security, shared personal groups (not reported by the Salesforce API), frozen users, and KB articles item permissions (see Unsupported Security Aspects).</td>
</tr>
<tr>
<td>security</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

www.coveo.com
• View All permissions

The Salesforce connector fully supports all View All permissions given through a user profile, more explicitly View All Data which applies to every object, View All User which allows a view all on the user object, and View All on specific objects such Accounts, Cases, Leads, and Contact.

**Note:** As Salesforce does not support View All Data on ContentVersion, the permission is replicated in the connector.

• Sharing permissions

An administrator can secure private objects with the owner, collaboration group, group, user, bosses of a given user, subordinates of a given user, or Community (also called Network) sharing permission types.

**Note:** CES 7.0.8225+ (March 2016) Portal Super User permissions are supported by the connector.

• Profile associated to the user

The profile specifies standard and custom object permissions for users associated to this profile.

**Note:** Any user which is granted Read access for an object by his profile is entitled to search for records of the given type.

• Organization-wide defaults sharing settings

These settings specify the level of access your users have to each other's data.

**Note:** CES 7.0.8388+ (June 2016) The external sharing model (organization-wide defaults) is supported by the connector.

• Shared content

A user can share private content with specific users or groups.

**Note:** File sharing settings applied to Chatter files and CRM Content documents are also supported. File sharing settings are not the same as the sharing settings for private objects.

• CRM Content

CRM Content users have access to CRM Content Documents when they are entitled to read such documents in the library to which the documents belong.

• Chatter

Chatter posts and comments inherit the permissions of the record onto which they are posted, no matter if that record is public, private, a group or a user.

**Note:** Public and private CollaborationGroups are supported.

• Communities

Sharing sets are supported in Communities.
- Role hierarchy within the organization

  With a role hierarchy, private documents are visible by the owner, but also by all parents of the owner in the hierarchy.

- Permission sets

  Permission sets given to individual users can extend (not restrict) their permissions beyond what is specified in their profile.

- License type

  A user license entitles a user to different functionality within Salesforce and determines which profiles and permission sets are available to the user, so the Coveo index indirectly replicates user license type permissions by indexing permissions from profiles and permission sets.
**Note:** The connector does not support the following security aspects:

- **Apex managed sharing**
- **IP based permissions**
  
  The Coveo connector cannot index restrictions on login IP addresses or hours configured in Salesforce. The consequence is that your Salesforce users can access Coveo search interfaces and review Salesforce content from any IP address at any time.
- **Field level security (FLS)**
  
  For Enterprise, Unlimited, and Developer Salesforce editions, visibility of individual fields can be granted or denied to users or groups to fine-tune the access control in a permission set or a profile. The Coveo connector cannot index these permissions. The consequence is that a user that is denied access to a field could see the content of this field in Coveo search results. Note however that this is also the case for Salesforce search results (see the Salesforce document [Field-Level Security Overview](https://help.salesforce.com/CS-FLS)).
- **Permission changes replicated with re-indexing, not with incremental refreshes**
  
  When permissions change in Salesforce for a profile, permission set, object sharing, or object security level (Public versus Private), the changes are not replicated in the index on the next incremental refresh. You must refresh the source to capture permission changes.
- **Shared personal groups**
  
  A user can share content with a personal group. These sharing permissions cannot be indexed because they are currently not reported by the Salesforce API. The consequence is that members of the personal group will not see the shared content in Coveo Organization results. This limitation is therefore not a security hole.
- **Frozen users are not supported**
  
  The user that are frozen using the **Freeze** button are not denied access to the search (see [Freezing User Accounts](https://help.salesforce.com/CS-FRO)).
- **Knowledge Base (KB) item permissions**:
  
  In Salesforce, you can map User Roles to KB data categories (e.g.: members of the Technical Agent role can only see KB articles under the Technical data category). This mapping information is not available from the Salesforce API and therefore cannot be indexed. Similarly, the permissions given through permission sets to grant only some users access to only one Article Type cannot be retrieved through the Salesforce API.
  
  Consequently, in search results, all users can see all KB articles under all data categories.
- **Sharing Default Access Settings**
  
  When the organization-wide default is set to Controlled by Parent, a maximum master-detail relationship depth of two levels is supported (see [Sharing Default Access Settings](https://help.salesforce.com/CS-SHAR)).

**Example:** When you index a subdetail object, the detail parents are correctly determined but the master parents are considered public because there are three levels (master-detail-subdetail).
Incremental Refresh

The incremental refresh feature refreshes the content of the index based on the modification date of the objects in the Salesforce environment. If an item is modified, the incremental refresh feature refreshes the item automatically.

Notes:

- The incremental refresh feature limitations:
  - Does not work when the last incremental refresh was performed more than 30 days ago. This will trigger a full refresh of the content.
  - Not supported for all not replicateable deleted objects such as deleted ContentVersion (CRM Content and Chatter files) attachments and other items.
  - **CES 7.0.7914– (October 2015)** A source full refresh or rebuild is needed to capture the deletion of knowledge base articles and the attachment (or the contrary) of articles on a case.

- **CES 7.0.8047+ (December 2015)** After you upgrade CES, it is recommended to perform a full refresh of your source(s) containing KB articles to take account of possible URI changes. You will also possibly have to change the ObjectsToGet configuration file depending on your needs (see Salesforce Connector Configuration Recipes). These modifications allow the connector to fully support the incremental refresh as well as the publish status changes of KB articles using stable URIs now produced by default.

- **CES 7.0.7914– (October 2015)** Stable URIs can only be produced with the help of Coveo Support for the latest version of online articles when draft and archived articles are not indexed.

Customizable ObjectsToGet Configuration File

You can customize items that the Coveo crawler retrieves from Salesforce (see "Creating a Salesforce ObjectsToGet Configuration File" on page 1472).

Customizable Mapping File

You can customize how the fields of Salesforce objects are mapped to searchable fields in the Coveo index (see "Creating a Salesforce Mapping File" on page 1505).

Feature History

<table>
<thead>
<tr>
<th>Coveo Platform version</th>
<th>Date</th>
<th>Features</th>
</tr>
</thead>
<tbody>
<tr>
<td>7.0.8047</td>
<td>December 2015</td>
<td>Full support of incremental refreshes on knowledge articles and indexing their publish status</td>
</tr>
<tr>
<td>7.0.7183</td>
<td>November 2014</td>
<td>Support validating the ObjectsToGet with an XSD [more]</td>
</tr>
<tr>
<td>Coveo Platform version</td>
<td>Date</td>
<td>Features</td>
</tr>
<tr>
<td>------------------------</td>
<td>----------------</td>
<td>-----------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>7.0.6767</td>
<td>June 2014</td>
<td>• Support incremental modification of knowledge base articles versions and states [more]</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Support incremental modification of user profiles</td>
</tr>
<tr>
<td>7.0.6424</td>
<td>February 2014</td>
<td>Knowledge content searchable by article number without inputting leading zeroes</td>
</tr>
<tr>
<td>7.0.6339</td>
<td>January 2014</td>
<td>• Partial incremental refresh support on knowledge articles</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Support multilingual knowledge articles</td>
</tr>
<tr>
<td>7.0.6196</td>
<td>November 2013</td>
<td>Adding support to crawl Chatter feed items and files.</td>
</tr>
<tr>
<td>7.0.5785</td>
<td>August 2013</td>
<td>Introduction of this second generation Salesforce connector</td>
</tr>
</tbody>
</table>

What’s Next?

Review the deployment process for the Salesforce connector (see "Salesforce Connector Deployment Overview" on page 1446).

9.38.4 Salesforce Connector Deployment Overview

The following procedure outlines the steps needed to index a Salesforce source. The steps indicate the order in which you must perform configurations tasks. When needed, the steps refer to a detailed procedure.

The Salesforce connector can index various Salesforce content types:

• Service Cloud standard and custom objects and fields

• Knowledge base articles

• Chatter

• CRM Content

When you want to index more than one of these Salesforce content types, you must use the following procedure to create a configuration (ObjectsToGet configuration file, mapping file, and source) for each of them because they cannot share the same set of configuration parameters.

To deploy the Salesforce connector

1. Validate that your environment meets the requirements (see "Salesforce Connector Requirements" on page 1448).

2. Configure the user identity
The Coveo connector needs an account to connect to your Salesforce organization and access the entire content that you want to index. You must create a CES user identity to hold the credentials of this Salesforce account (see "Creating a Salesforce User Identity" on page 1449).

3. Get Salesforce Client_ID and Client_Secret values

The Coveo security provider and connector for Salesforce must know the Client_ID and Client_Secret values for your Salesforce organization to be authorized to access its content (see "Getting Salesforce Client_ID and Client_Secret Values" on page 1453).

4. Create an ObjectsToGet configuration file

An ObjectsToGet XML configuration file tells the crawler which Salesforce items to retrieve (see "Salesforce ObjectsToGet Configuration File" on page 1457).

You must create your custom ObjectsToGet XML configuration file before configuring your source. You can create the file based on examples that include standard objects and include your custom objects (see "Creating a Salesforce ObjectsToGet Configuration File" on page 1472).

5. Configure a mapping file

A Salesforce source needs a mapping file to know how to map retrieved Salesforce items to CES index fields. You must create a mapping file before you configure your Salesforce source (see "Creating a Salesforce Mapping File" on page 1505).

6. Create a custom Salesforce field set

   a. The Salesforce source needs a field set matching the CES fields that are included in the mapping file. It is recommended to start by importing the default Salesforce field set file (\[CES_Path]\Bin\Coveo.CES.CustomCrawlers.Salesforce.FieldSet.xml) to create fields for all the metadata available by default from Salesforce content.

   b. When you created custom Salesforce object and fields, add corresponding fields to the field set.

7. Configure an Email security provider

   **Note:** For a Salesforce Knowledge Base source, you do not need to perform this procedure. Knowledge Base permissions cannot be indexed so no Email security provider is needed.

In Salesforce, users are identified by their email addresses. Consequently, permissions returned by the Salesforce security provider for each document are email addresses. The Salesforce security provider then requires another security provider to uniquely identify users from their email addresses.

The security provider type to use depends on how users are authenticated when they access the search interface:

- When authenticated with their email address, use an Email security provider (see "Configuring an Email Security Provider" on page 65).

- When authenticated with their Active Directory account, use an Active Directory security provider (see "Configuring an Active Directory Security Provider" on page 1141).
**Note:** An Active Directory security provider is appropriate only when the User Principal Name (UPN) matches the email address for all users.

**Note:** You may require to also use a Regex Transform Member Name security provider in between the two other security providers to map member types. Contact Coveo Support for assistance.

8. Configure a Salesforce security provider

**Note:** For a Salesforce Knowledge Base source, you do not need to perform this procedure. Knowledge Base permissions cannot be indexed so no Email security provider is needed.

A Salesforce source needs a Salesforce security provider (see "Configuring a Salesforce Security Provider" on page 1534).

9. Configure and index the Salesforce source

The Coveo connector needs to know details about your Salesforce organization to be able to index the desired content (see "Configuring and Indexing a Salesforce Source" on page 1536).

10. If you encounter issues:

- Solve typical issues that return error messages (see "Troubleshooting Salesforce Connector Issues" on page 1546).
- Consider adding and modifying default values of hidden source parameters (see "Modifying Hidden Salesforce Source Parameters" on page 1543).

### 9.38.5 Salesforce Connector Requirements

Your environment must meet the following requirements to be able to use the Coveo connector for Salesforce repositories:

- **CES 7.0.5785+ (August 2013)**

- Coveo for Salesforce license
  
The Salesforce connector is only available on-premises if you have acquired a suitable Coveo for Salesforce license (see Coveo for Salesforce).

- **Note:** You can see if the Salesforce connector is enabled in your CES 7.0 instance from the CES Administration Tool.

- An active Salesforce account to a Salesforce organization
  
The crawling account must have permissions to read all the types of content that you want to index (see "Creating a Salesforce User Identity" on page 1449).

### What's Next?

Create a user identity to be used by the Coveo connector to crawl your Salesforce content (see "Creating a Salesforce User Identity" on page 1449).
9.38.6 Creating a Salesforce User Identity

The Coveo connector and security provider for Salesforce must use a user account to connect to your Salesforce organization.

When an application such as the Coveo connector accesses your Salesforce content through the API, it must provide credentials where the Security Token associated to the account is appended to the password.

**Important:** Salesforce may regularly request a password change which will generate a new Security Token at the same time. You must then each time update the user identity with the new password and Security Token.

To create a Salesforce user identity

1. In the Salesforce organization that you want to index:
   a. Select or create an account to be used by the Coveo connector and security provider to access your Salesforce content (see "Creating a Dedicated Salesforce Crawling Account" on page 1450).
   b. Find the Salesforce Security Token for this account (see "Getting the Security Token for Your Salesforce Account" on page 1452).
2. On the Coveo server, access the Administration Tool.
3. In the Administration Tool, select **Configuration > Security**.
4. In the navigation panel on the left, select **User Identities**.
5. In the **User Identities** page, click **Add**.
6. In the **Modify User Identity** page:

   ![Modify User Identity](image)

   a. In the **Name** box, enter a name for this user identity.

   **Example:** Salesforce Crawling Account

   ![Example](image)
b. In the **User** box, enter the user name of the selected Salesforce account, typically the email address.

c. In the **Password** box, enter the password to which you append the Security Token for the selected Salesforce account with no space in between.

**Example:** When the password is **ThisIsMyPassword** and the Security Token is **DU5PJU3GtHbQaX0zxiWoCMq8Z**, then enter **ThisIsMyPasswordDU5PJU3GtHbQaX0zxiWoCMq8Z**.

d. Click **Apply Changes**.

What’s Next?

Your Salesforce source and security provider will need to know the **Client_ID** and **Client_Secret** values for your Salesforce organization (see "Getting Salesforce Client_ID and Client_Secret Values" on page 1453).

9.38.6.1 Creating a Dedicated Salesforce Crawling Account

The Coveo connector can use a Salesforce administrator account to access and crawl your Salesforce content. It is however a better practice to create dedicated Salesforce user, profile, and permission set for the Coveo crawling, that specify minimal permissions and access.

**Note:** It is strongly recommended to have separate dedicated Salesforce crawling accounts for each Salesforce source and security provider. When the Coveo crawler accesses Salesforce with the same user credentials too many times, Salesforce returns **INVALID_QUERY_LOCATOR** error messages, such as the following:

*Error with ID 'SALESFORCE_INVALID_QUERY': invalid query locator (INVALID_QUERY_LOCATOR)*

- This error can occur if a user is used more than once for sources that run in parallel. To avoid this error, make sure to use only one user per source or alternate the refresh schedule of your sources.

To create a dedicated Salesforce crawling account

1. Using an administrator account, log in to your Salesforce organization.

2. In the user menu, select **Setup**.

3. Create a Salesforce profile dedicated to the Coveo crawler:

   a. In the **Setup** page, select **Manage Users > Profiles**.

   b. In the **Profiles** page, click **New Profile**.

   c. In the **Clone Profile** page:
### Clone Profile

Enter the name of the new profile.

<table>
<thead>
<tr>
<th>You must select an existing profile to clone from.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Existing Profile: Read Only</td>
</tr>
<tr>
<td>User License: Salesforce</td>
</tr>
<tr>
<td>Profile Name: CoveoIndexer</td>
</tr>
</tbody>
</table>

**i.** In the *Existing Profile* box, select an existing profile such as *Read Only* to be used as a template for the new profile according to the permissions you want to grant to the crawler.

**ii.** In the *Profile Name* box, enter a name such as *CoveoIndexer*.

**iii.** Click *Save*.

**d.** In the page for your new profile, click *Edit* and in the *Administrative Permissions* section:

**i.** Ensure that the *API Enabled* option is selected.

**ii.** Optionally, select the *API Only User* option as an additional security measure.

**iii.** Select the *Modify All Data* option when any of the following situation applies:

- You are using **CES 7.0.6225–(December 2013)** or prior.
- You want to index the Salesforce item permissions.

**Note:**

- The *Modify All Data* permission is required because the Salesforce permissions can be indexed only through the Salesforce Metadata API that is only accessible with the *Modify All Data* permission.
- If you do not enable *Modify All Data*, be aware that the crawler will only index content to which it has access, so set up read access to objects accordingly.

**iv.** When indexing Knowledge content, ensure that **Knowledge User** is checked.

**v.** Optionally, as an additional security measure, in the *Login IP Ranges* section, select or create a login IP range to restrict the accessibility for this profile (see **Coveo Platform IP address range**).

4. Create a Salesforce user dedicated to the Coveo crawler:
a. In the Setup page, select **Manage Users** > **Users**.

b. In the **All Users** page, click **New User**.

c. In the **New User** page:
   i. Fill the required fields.
   ii. In the **Profile** box, select the profile you just created.
   iii. Click **Save**.

9.38.6.2 Getting the Security Token for Your Salesforce Account

When you create a Salesforce account, Salesforce sends an email message from support@salesforce.com with subject: **salesforce.com security token confirmation** to the email address associated with the account. This email message contains the Security Token for the account and is the only place where you can find the Security Token value. When you change the account password, the security token is also regenerated (so the previous one expires) and a similar email is sent.

To get the security token for your Salesforce account

1. In the mailbox for the email address associated with the Salesforce account to be used by the Coveo connector, look for the latest email message received from support@salesforce.com with subject: **salesforce.com security token confirmation**.

2. If you cannot find the latest email with security token, reset the security token:
   a. Log in to Salesforce using the Salesforce account to be used by the Coveo connector.
   b. In the User Menu, select **Setup**.
   c. In the menu on the left, under **Personal Setup**, expand **My Personal Information**, and then click **Reset My Security Token**.
   d. Follow onscreen instructions.

   A new email message will be sent.

3. Open the message, and then copy the Security Token value.
Example: In the following email example, the Security Token value is highlighted.

```
Your Security Token is Enclosed.

Dear MyName,

When accessing salesforce.com from outside of your company’s trusted networks, you must add a security token to your password to log in to a desktop client, such as Connect for Outlook, Connect Offline, Connect for Office, Connect for Lotus Notes, or the Data Loader.

New security tokens are automatically sent to you when your salesforce.com password is changed or when you request to reset your security token.

Your new security token is below. Note that security tokens are case sensitive.

User Name: MyName@MyCompany.com
Security Token: 3U5PU3G8hQaX0z0iWoCMqiz

Please add your security token to your password. Note that you do not enter a security token in place of your password when logging into salesforce.com via a browser.
```

9.38.7 Getting Salesforce Client_ID and Client_Secret Values

The Force.com platform implements the OAuth 2.0 Authorization Framework, so users can authorize applications to access Force.com resources.

When you configure the Coveo Salesforce security provider and Salesforce source, you must know the Client_ID and Client_Secret token values for the Salesforce organization that you want to index.

To get the Salesforce Client_ID and Client_Secret values

1. Using and administrator account, log into the Salesforce organization that you want to index.
2. On the User Menu, select Setup.
3. In the navigation menu on the left, under App Setup, expand Create, and then click Apps.
4. In the Apps page, in the Connected Application section, click New to create a new application that will use OAuth2 to gain access to the organization.
5. In the New Connected App page:
a. In the **Basic Information** section:

   i. Enter meaningful names in the **Connected App Name** and **API Name** boxes.

   ii. Enter your email in the **Contact Email** box so that you can receive messages from this application.

b. In the **API (Enable OAuth Settings)** section:

   i. Select the **Enable OAuth Settings** check box.

   ii. In the **Callback URL** box, since a callback URL will not be used for this application, enter a dummy but valid secured URL (https://) such as https://login.salesforce.com/services/oauth2/callback.

   iii. In the **Available OAuth Scopes** list, select the following items:
• Access and manage your data (api)
• Full access (full)
• Perform requests on your behalf at any time (refresh_token, offline_access)

and click Add for each so that they appear in the Selected OAuth Scopes list.

c. Click Save.

6. In the page that appears for your new connected app, in the API (Enable OAuth Settings) section:

   ![API Settings](image)

   a. Copy the Consumer Key value and paste it in a secure reference document of your choice.

   The Consumer Key is the client_id.

   b. Next to Consumer secret, click Click to reveal, copy the value that appears, and then paste it in your secure reference document.

   The Consumer secret is the client_secret.

   c. Save your reference document.

   **Note:** You can always come back to this Salesforce page (Setup > App Setup > Create > Apps, and clicking the application name in the Connected Apps list).

7. Create a Salesforce permission set dedicated to the Coveo crawler and assign it to your dedicated app and user:

   a. In the Setup page, select Manage Users > Permission Sets.

   b. In the Permission Sets page, click New.

   c. In the Create page, in the Label and API Name boxes, enter significant names, and then click Save.
d. In the page for the new permission set:

i. Click Manage Assignments, and then add the dedicated user you created earlier for the Coveo crawler (see "Creating a Dedicated Salesforce Crawling Account" on page 1450).

ii. In the Apps section, click Assigned Connected Apps.

iii. In the Assigned Connected Apps section, click Edit. add the connected app you just created to the
What's Next?

Create an ObjectsToGet Configuration file (see “Salesforce ObjectsToGet Configuration File” on page 1457).

9.38.8 Salesforce ObjectsToGet Configuration File

The ObjectsToGet configuration file of the Salesforce connector contains the definition of all standard or custom objects that will be retrieved from the Salesforce organization. Each object definition is used to generate the SOQL query executed by the connector to retrieve the records for that object.

With this configuration file, you get control over:

- Which information is retrieved by specifying the fields and relationships that should be fetched for each object. This information will be available to use in the mapping file.
- Which records are returned by specifying conditions on the SOQL query that will be used to filter the query results.
Notes:

- If you want to retrieve Salesforce Knowledge Base articles, you need to specify at least two queries for each type of Knowledge article, one for the *__ka object and one the *__kav object (see “Salesforce ObjectsToGet Configuration File Example for Knowledge Base” on page 1485).

- There is a bug in the Salesforce API that causes the returned JSON to be invalid when querying a binary field of an object, so ensure to not include any binary field in your query.

  **CES 7.0.7914+ (October 2015)** Support for the * character to replace a list of Objects and Parent relationship fields that are queryable.

  **Example:** When the mapping file contains the following:

  ```xml
  <Query>
  <ObjectName>Case</ObjectName>
  <Fields>
  <string>*</string>
  </Fields>
  </Query>
  ```

  You can use the following SOQL query: `<Query value="Select * from Case" />`

  **CES 7.0.8047+ (December 2015)** Support for the * character to replace a list of Child relationship fields that are queryable.

  **Example:** `<Query value="Select *,Parent.*, (Select * from Children) From Object/"/>

9.38.8.1 Salesforce Object Definition

To obtain the list of queryable fields on a specific object:

- Salesforce developers can use the describeSObject() method to obtain the complete object definition in JSON format.

  **Example:** https://na15.salesforce.com/services/data/v27.0/objects/Account/describe

- Salesforce administrators can obtain the complete list of fields from Salesforce API online documentation (see Account, Task).

To obtain the list of available relationships on a specific object:

- Salesforce administrators can access any object definition from Salesforce in the **Setup** under the **Customize** menu. Object relationships are identified by fields of data type **Lookup** (see AccountFields, TaskFields).

9.38.8.2 Configuration File Elements

The ObjectsToGet Salesforce configuration file is an aggregate of query XML nodes. A query node contains several elements, each one being used to generate the SOQL query of a Salesforce object.

**Value attribute (optional)**

  **CES 7.0.7814+ (August 2015)**

  You can specify an SOQL query in the query value as shown in the following example (see Salesforce Object
Query Language (SOQL):

```
<Query value="Select Id, Owner.Id, (Select Id From Shares) From Case Where CaseNumber>10" />
```

Keep in mind that only what is already in the objects to get is supported.

**ObjectName (required)**

The name of the object (standard or custom) to query (see Standard Objects).

*Note: If you are using the value attribute, the object name is optional and must be the same.*

**GroupBy (optional)**

The name of the field on which results should be grouped by.

**Limit (optional)**

The maximum number of items that will be retrieved by the query.

**Offset (optional)**

The number of items that should be skipped in query results.

**Fields (required)**

Contains the name of the fields (Field Name column in Salesforce) that will be available on each record returned by the query. Each field name must be in a `<string>` element, no matter its data type. Fields specified in this section can be of any data type except Lookup.

**Example:**

```
<Query>
  <ObjectName>Account</ObjectName>
  <Fields>
    <string>Id</string>
    <string>IsDeleted</string>
    <string>Name</string>
    <string>Type</string>
    <string>BillingStreet</string>
    <string>BillingCity</string>
    <string>BillingState</string>
    <string>BillingPostalCode</string>
    <string>BillingCountry</string>
    <string>Phone</string>
    <string>Fax</string>
    <string>AccountNumber</string>
    <string>Website</string>
    <string>Sic</string>
    <string>Industry</string>
    <string>AnnualRevenue</string>
    <string>NumberOfEmployees</string>
    <string>Ownership</string>
    <string>TickerSymbol</string>
    <string>Description</string>
    <string>Rating</string>
    <string>Site</string>
    <string>CreatedDate</string>
    <string>LastModifiedDate</string>
    <string>SystemModstamp</string>
  </Fields>
</Query>
```
QueryCondition (optional)

Important: CES 7.0.6942– (August 2014) This operator is not validated and has a free form. However, the resulting SOQL must be in the format FIELD OPERATOR VALUE. Rather use QueryCondition2.

One or more conditions that will be applied to the SOQL query used to retrieve object records.

- **Field (required):**
  
  Case-insensitive name of the object field on which the condition is applied. Relationship names can also be used (ex: Parent.Type).

- **Operator (required):**
  
  The operator to apply to the condition. Any operator supported by Salesforce SOQL queries can be used (see Comparison Operators).

- **Value (required):**
  
  Case-sensitive value used to evaluate the condition. String values must be enclosed in single quotes.

**Example:**

```xml
<Query>
  <ObjectName>Account</ObjectName>
  <Fields>
    <string>Name</string>
    <string>AccountNumber</string>
  </Fields>
  <Conditions>
    <QueryCondition>
      <Field>Type</Field>
      <Operator>!=</Operator>
      <Value>'Prospect'</Value>
    </QueryCondition>
    <QueryCondition>
      <Field>Owner.Name</Field>
      <Operator>=</Operator>
      <Value>'John Smith'</Value>
    </QueryCondition>
  </Conditions>
</Query>
```

The generated query is:

```
SELECT Name FROM Account WHERE Type != 'Prospect' AND Owner.Name = 'John Smith'
```

QueryCondition2 (optional)

**Note:** This query condition is validated and has more options. This is the preferred way to create a query condition.

One or more conditions that will be applied to the SOQL query used to retrieve object records.

- **Field (required):** Case-insensitive name of the Object Field on which the condition is applied. Relationship names can also be used (e.g. Parent.Type).

- **Relation (required):** The operator to apply to the condition. Supported operators are Equal, NotEqual,
Less, LessOrEqual, Greater, GreaterOrEqual, Like, NotLike.

- **SoqlString|SoqlBoolean|SoqlDateTime** *(required): Case-sensitive value (not Like) used to evaluate the condition.*

**Example:**

```xml
<Query>
  <ObjectName>Account</ObjectName>
  <Fields>
    <string>Name</string>
  </Fields>
  <Conditions>
    <QueryCondition2>
      <Field>Type</Field>
      <Relation>NotEqual</Relation>
      <SoqlString>Prospect</SoqlString>
    </QueryCondition2>
    <QueryCondition2>
      <Field>IsEscalated</Field>
      <Relation>Equal</Relation>
      <SoqlBoolean>true</SoqlBoolean>
    </QueryCondition2>
    <QueryCondition2>
      <Field>LastViewDate</Field>
      <Relation>GreaterOrEqual</Relation>
      <SoqlDateTime>2014-04-28T00:00:00.0000000-00:00</SoqlDateTime>
    </QueryCondition2>
  </Conditions>
</Query>
```

**Note:** For **SoqlDateTime**, the date/time format must exactly match `YYYY-MM-DDTHH:MM:SS.0000000-00:00`

The generated query is:

```
SELECT Name FROM Account WHERE Type != 'Prospect' AND IsEscalated = true AND LastViewDate >= 2014-04-28T00:00:00
```

**InCondition (optional)**

- **Field** *(required): Case-insensitive name of the Object Field on which the condition is applied. Relationship names can also be used (e.g. Parent.Type).*

- **AllowedValues** *(required): Case-sensitive possible values of the field.*
Example:

```
<Query>
  <ObjectName>Account</ObjectName>
  <Fields>
    <string>Name</string>
  </Fields>
  <Conditions>
    <InCondition>
      <Field>Type</Field>
      <AllowedValues>
        <SoqlString>Prospect</SoqlString>
        <SoqlString>Client</SoqlString>
      </AllowedValues>
    </InCondition>
  </Conditions>
</Query>
```

The generated query is:

```
SELECT Name FROM Account WHERE Type IN ('Prospect', 'Client')
```

**InQueryCondition (optional)**

**CES 7.0.7183+ (November 2014) Semi-joins are supported in query's conditions (see Comparison Operators).**

Semi-joins are useful when you want to index only a subset of records based on another set of records.

- **Field (required):**
  Case-insensitive name of the object field on which the condition is applied. Relationship names can also be used (ex.: Parent.Type).

- **Query (required): A valid query object (with ObjectName, Fields, etc) (see Semi-Joins or Anti-Joins Relationship Query Limits).**
Example:

```xml
<Query>
  <ObjectName>Case</ObjectName>
  <Fields>
    <string>Id</string>
  </Fields>
  <Conditions>
    <InCondition>
      <Field>Id</Field>
      <Query>
        <ObjectName>CaseComment</ObjectName>
        <Fields>
          <string>ParentId</string>
        </Fields>
        <Conditions>
          <QueryCondition>
            <Field>CommentBody</Field>
            <Operator>=</Operator>
            <Value>'this is a test'</Value>
          </QueryCondition>
        </Conditions>
      </Query>
    </InCondition>
  </Conditions>
</Query>
```

The generated query is:

```
SELECT Id FROM Case WHERE Id IN (SELECT ParentId FROM CaseComment WHERE CommentBody = 'this is a test')
```

Not InQueryCondition (optional)

CES 7.0.7183+ (November 2014) Anti-joins are supported in query's conditions (see Comparison Operators). Anti-joins are useful when you want to index only a subset of records based on another set of records.

- **Field (required):**
  
  Case-insensitive name of the object field on which the condition is applied. Relationship names can also be used (ex.: Parent.Type).

- **Query (required):** A valid query object (with ObjectName, Fields, etc) (see Semi-Joins or Anti-Joins Query Limits).
Example:

```
<Query>
  <ObjectName>Case</ObjectName>
  <Fields>
    <string>Id</string>
  </Fields>
  <Conditions>
    <NotCondition>
      <InCondition>
        <Field>Id</Field>
        <Query>
          <ObjectName>CaseComment</ObjectName>
          <Fields>
            <string>ParentId</string>
          </Fields>
          <Conditions>
            <QueryCondition>
              <Field>CommentBody</Field>
              <Operator>='this is a test'</Operator>
              <Value>'this is a test'</Value>
            </QueryCondition>
          </Conditions>
        </Query>
      </InCondition>
    </NotCondition>
  </Conditions>
</Query>
```

The generated query is:

```
SELECT Id FROM Case WHERE NOT Id IN (SELECT ParentId FROM CaseComment WHERE CommentBody = 'this is a test')
```

**ParentRelationship (optional)**

One or more relationships which information will be available on each object record returned by the query. An object relationship is defined by a lookup field which creates a relation between the current object being queried and another object. These relations allow SOQL query operations similar to SQL joins.

- **RelationshipName (required):**
  The field name of data type Lookup.

- **Fields (required):**
  The name of the fields of the related object that will be available on each record returned by the query.

- **ParentRelationships (optional):**
  Another level of parent relationship, but this time, the relationship applies to the related object.
Example:

```xml
<Query>
  <ObjectName>Account</ObjectName>
  <Fields>
    <string>Name</string>
    <string>AccountNumber</string>
  </Fields>
  <ParentRelationships>
    <ParentRelationship>
      <RelationshipName>Owner</RelationshipName>
      <Fields>
        <string>Name</string>
        <string>Email</string>
      </Fields>
    </ParentRelationship>
  </ParentRelationships>
</Query>
```

Important: The parent field is copied to the record. If the parent is modified, the indexed record is not updated.

**ChildRelationship (optional)**

One or more relationships which information will be available on each **Object** record returned by the query. An **Object** relationship is defined by a Lookup Field which creates a relation between the current **Object** being queried and another **Object**. These relations allow SOQL query operations similar to SQL joins.

- **Query (required): A valid query object (with **ObjectName**, **Fields**, etc).**

Example:

```xml
<Query>
  <ObjectName>Opportunity</ObjectName>
  <Fields>
    <string>Id</string>
    <string>Name</string>
  </Fields>
  <ChildRelationships>
    <Query>
      <ObjectName>Attachments</ObjectName>
      <Fields>
        <string>Id</string>
        <string>Name</string>
      </Fields>
    </Query>
  </ChildRelationships>
</Query>
```

The generated query is:

```
SELECT Id, Name, (SELECT Id, Name FROM Attachments) FROM Opportunity
```

The generated metadata, when an attachment is found on the opportunity:

```
"Attachments.attribute.type" => "Attachment"
"Attachments.attribute.url" => "/services/data/v29.0/objects/Attachment/00PG000000B8RUvMAN"
"Attachments.Id" => "00PG000000B8RUvMAN"
"Attachments.Name" => "a_stash_of_werthers.jpg"
```
**Note:**

- When more than one child exist, the fields contain values separated with a semicolon.

  Example: `Attachments.Name: a.jpg;b.jpg`

- Nested child relationships (sub-sub queries) are not supported.

**Important:** CES 7.0.8850– (March 2017) The child field is copied to the record. If a child is modified, the indexed record is not updated.

**CreateRecord (optional)**

CES 7.0.8996+ (June 2017) To be used only inside a ChildRelationship. It creates an item from child records.

In the following example, Attachments from Opportunities are created as items in the Coveo index.

**Example:**

```
<Query>
  <ObjectName>Opportunity</ObjectName>
  <Fields>
    <string>Id</string>
    <string>Name</string>
  </Fields>
  <ChildRelationships>
    <ChildRelationship>
      <RelationshipName>Attachments</RelationshipName>
      <Fields>
        <string>Id</string>
        <string>Name</string>
      </Fields>
      <CreateRecord>true</CreateRecord>
    </ChildRelationship>
  </ChildRelationships>
</Query>
```

**PolymorphicRelationship (optional)**

Polymorphic relationships can be useful for parent relationships on a Lookup field that can be related to multiple types of objects (ex: Lookup (Contract, Campaign, Account, Opportunity, Product, Asset, Case, Solution)). The polymorphic relationship allows for different fields to be retrieved depending on the object that will be related for a specific record.
Notes:

- **CES 7.0.8047+ (December 2015)** Polymorphic relationships no longer depend on a parent relationship to work.

  **Example:** You can add the following on feed items (TextPost, LinkPost, ContentPost, PollPost) to create the CreatedBy.SmallPhotoUrl metadata when indexing FeedItem, FeedComment and collaborationgroup:

  ```xml
  <PolymorphicRelationship>
  <RelationshipName>CreatedBy</RelationshipName>
  <ObjectName>User</ObjectName>
  <Fields>
    <string>Name</string>
    <string>Type</string>
    <string>PhotoURL</string>
  </Fields>
  </PolymorphicRelationship>
  ``

- The two following metadata appear on the record with polymorphic relationships: `<polymorphic_relationship_name>.<field>` and `<polymorphic_relationship_name>_<object_name>.<field>`.

- **CES 7.0.7104— (October 2014)** The record with polymorphic relationships only provided the metadata named `<polymorphic_relationship_name>_<object_name>.<field>`.

- **FieldName (required):**
  The field name of data type Lookup.

- **ObjectName (optional):**
  The related object type this polymorphic relationship applies to.

  **Note:** **CES 7.0.7104— (October 2014)** The ObjectName field is required.

- **Fields (required):**
  The name of the fields of the related object that will be available on each record returned by the query.

- **ParentRelationships (optional):**
  Another level of parent relationship, but this time, the relationship applies to the related object.
Example:

```xml
<Query>
  <ObjectName>Task</ObjectName>
  <Fields>
    <string>Id</string>
    <string>Subject</string>
    <string>ActivityDate</string>
  </Fields>
  <ParentRelationships>
    <ParentRelationship>
      <RelationshipName>What</RelationshipName>
      <Fields>
        <string>Name</string>
        <string>Type</string>
      </Fields>
    </ParentRelationship>
  </ParentRelationships>
  <PolymorphicRelationships>
    <PolymorphicRelationship>
      <RelationshipName>What</RelationshipName>
      <ObjectName>Account</ObjectName>
      <Fields>
        <string>Name</string>
        <string>AccountNumber</string>
      </Fields>
    </PolymorphicRelationship>
    <PolymorphicRelationship>
      <RelationshipName>What</RelationshipName>
      <ObjectName>Opportunity</ObjectName>
      <Fields>
        <string>Amount</string>
        <string>TotalOpportunityQuantity</string>
      </Fields>
    </PolymorphicRelationship>
  </PolymorphicRelationships>
</Query>
```

Important: The parent field is copied to the record. If a parent is modified, the indexed record is not updated.

Order (optional) CES 7.0.6607+ (April 2014)

One or more order restrictions that will be applied to the SOQL query used to retrieve Object records.

- **Ascending (optional):** The direction of the ordering. Default is true (ascending). Use `false` for descending.
- **NullsFirst (optional):** Whether records with NULL values in the specified fields must be returned first or last. Default is true.
- **Fields (required):** One or more fields to base the ordering on, in the specified field order.
Examples:

With the following configuration:

- **Opportunity.Id** shows that we can specify the query object name as the parent of the field.

- **Account.Foo.Id** is a field on the parent Foo, which is also a field of the parent Account of Opportunity.

- **What.Id** is a field on the polymorphic parent What of Opportunity.

```
<Query>
  <ObjectName>Opportunity</ObjectName>
  <Fields>
    <string>Id</string>
  </Fields>
  <Order>
    <Ascending>true</Ascending>
    <NullsFirst>false</NullsFirst>
    <Fields>
      <string>Name</string>
      <string>Opportunity.Id</string>
      <string>Account.Foo.Id</string>
      <string>What.Id</string>
    </Fields>
  </Order>
</Query>
```

The generated query is:

```
SELECT Id FROM Opportunity ORDER BY Name, Opportunity.Id, Account.Foo.Id, What.Id ASC NULLS LAST
```

Configuration including a child relationship:

```
<Query>
  <ObjectName>Opportunity</ObjectName>
  <Fields>
    <string>Id</string>
  </Fields>
  <ChildRelationships>
    <Query>
      <ObjectName>Attachments</ObjectName>
      <Fields>
        <string>Id</string>
      </Fields>
      <Order>
        <Fields>
          <string>Name</string>
        </Fields>
      </Order>
    </Query>
  </ChildRelationships>
</Query>
```

The generated query is:

```
SELECT Id, (SELECT Id FROM Attachments ORDER BY Name ASC NULLS FIRST) FROM Opportunity
```
9.38.8.3 XML Schema Definition

Note: CES 7.0.7183+ (November 2014) Each of the ObjectsToGet in your Salesforce sources are validated against the XSD.

If it is not the case, a SALESFORCE_INVALID_CONFIGURATION error message appears in the CES console and logs.

Use the following XML schema definition to validate your configuration file.

```xml
<?xml version="1.0" encoding="utf-8"?>
<xs:schema id="ArrayOfQuery" xmlns="" xmlns:xs="http://www.w3.org/2001/XMLSchema"
 xmlns:msdata="urn:schemas-microsoft-com:xml-msdata">
  <xs:element name="Fields">
    <xs:complexType>
      <xs:sequence>
        <xs:element name="string" nillable="true" minOccurs="0" maxOccurs="unbounded">
          <xs:complexType>
            <xs:simpleContent msdata:ColumnName="string_Text" msdata:Ordinal="0">
              <xs:extension base="xs:string">\n                <xs:extension>
                  <xs:complexType>
                    <xs:sequence>
                      <xs:element name="RelationshipName" type="xs:string" minOccurs="0" maxOccurs="1"/>
                      <xs:element ref="Fields" minOccurs="0" maxOccurs="unbounded"/>
                    </xs:sequence>
                  </xs:complexType>
                </xs:extension>
              </xs:complexType>
            </xs:simpleContent>
          </xs:complexType>
        </xs:element>
      </xs:sequence>
    </xs:complexType>
  </xs:element>
  <xs:element name="ParentRelationships">
    <xs:complexType>
      <xs:sequence>
        <xs:element name="ParentRelationship" minOccurs="0" maxOccurs="unbounded">
          <xs:complexType>
            <xs:sequence>
              <xs:element name="RelationshipName" type="xs:string" minOccurs="0" maxOccurs="1"/>
              <xs:element ref="Fields" minOccurs="0" maxOccurs="unbounded"/>
            </xs:sequence>
          </xs:complexType>
        </xs:element>
      </xs:sequence>
    </xs:complexType>
  </xs:element>
  <xs:element name="Query" type="QueryType"/>
</xs:schema>
```
What's Next?

Create your ObjectsToGet configuration file (see "Creating a Salesforce ObjectsToGet Configuration File" on page 1472).
Creating a Salesforce ObjectsToGet Configuration File

You must create an ObjectsToGet configuration file and attach it to your Salesforce source to instruct the connector which objects to retrieve from your Salesforce organization (see "Salesforce ObjectsToGet Configuration File" on page 1457).

**Note:** You must be familiar with standard and custom objects and fields used in your Salesforce organization to be able to create a custom ObjectsToGet configuration file.

The content of the ObjectsToGet configuration file typically includes standard objects but most likely also the custom objects that you want to index. You can create your ObjectsToGet configuration file by starting with provided examples and customize it to suit your needs.

It is recommended to create separate ObjectsToGet configuration files with separate sources for the following types of Salesforce content:

- Service Cloud standard and custom objects and fields
- Knowledge base articles
- CRM Content

To create a Salesforce ObjectsToGet configuration file

1. Refer to the most appropriate of the following topics to copy the content of the corresponding ObjectsToGet XML configuration file example:
   - Salesforce ObjectsToGet Configuration File Example for Standard Objects
   - "Salesforce ObjectsToGet Configuration File Example for Knowledge Base" on page 1485
   - "Salesforce ObjectsToGet Configuration File Example for CRM Content" on page 1488

2. Using a text editor:
   a. Paste the content of the ObjectsToGet configuration file example.
   b. Modify or remove standard objects and fields, or add custom objects and fields to match the needs of your Salesforce organization (see "Salesforce ObjectsToGet Configuration File" on page 1457).
   c. Save your ObjectsToGet configuration file.

3. Validate your ObjectsToGet configuration file (see "XML Schema Definition" on page 1470).

4. Using an administrator account, connect to the Coveo Master server, and copy your custom ObjectsToGet configuration file to a location accessible to CES.

**Example:** On the Coveo Master server, for an ObjectsToGet configuration file for standard and custom objects and fields, save the file as:

`D:\CES7\Config\Salesforce_Basic_ObjectsToGet.xml`

You will specify the full path to this file when you configure your Salesforce source (see "ObjectsToGet File" on page 1539).
What's Next?

Create a mapping file to transfer the values of fields retrieved from Salesforce into CES fields (see “Creating a Salesforce Mapping File” on page 1505).

9.3.8.5.5 Salesforce ObjectsToGet Configuration File Example for Standard Objects

The ObjectsToGet configuration file example presented in this topic specifies to retrieve the following standard Service Cloud objects and fields (including Chatter feed items) that are typically useful to index:

- Account
- Case
- Case Comment
- Contact
- Event
- Solution
- Task
- User
- Attachment
- Feed item (Chatter) CES 7.0.6196+ (November 2013)
- Feed comment (Chatter) CES 7.0.6196+ (November 2013)

The following code sample is the content of the ObjectsToGet configuration file example for standard Service Cloud objects and fields.

```xml
<?xml version="1.0" encoding="utf-8"?>
<ArrayOfQuery xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns:xsd="http://www.w3.org/2001/XMLSchema">
  <Query>
    <ObjectName>Account</ObjectName>
    <Fields>
      <string>Id</string>
      <string>IsDeleted</string>
      <string>Name</string>
      <string>Type</string>
      <string>BillingStreet</string>
      <string>BillingCity</string>
      <string>BillingState</string>
      <string>BillingPostalCode</string>
      <string>BillingCountry</string>
      <string>Phone</string>
      <string>Fax</string>
      <string>AccountNumber</string>
      <string>Website</string>
      <string>Sic</string>
      <string>Industry</string>
      <string>Sic</string>
      <string>NumberOfEmployees</string>
      <string>Ownership</string>
      <string>TickerSymbol</string>
      <string>Description</string>
      <string>Rating</string>
    </Fields>
  </Query>
</ArrayOfQuery>
```
<string>Site</string>
<string>CreatedDate</string>
<string>LastModifiedDate</string>
<string>SystemModstamp</string>
<string>LastActivityDate</string>
<string>Jigsaw</string>
<string>JigsawCompanyId</string>
<string>AccountSource</string>
<string>SicDesc</string>
</Fields>
</ParentRelationships>
<ParentRelationship>
  <RelationshipName>MasterRecord</RelationshipName>
  <Fields>
    <string>Name</string>
  </Fields>
</ParentRelationship>
<ParentRelationship>
  <RelationshipName>Parent</RelationshipName>
  <Fields>
    <string>Name</string>
  </Fields>
</ParentRelationship>
<ParentRelationship>
  <RelationshipName>Owner</RelationshipName>
  <Fields>
    <string>Name</string>
  </Fields>
</ParentRelationship>
<ParentRelationship>
  <RelationshipName>CreatedBy</RelationshipName>
  <Fields>
    <string>Name</string>
  </Fields>
</ParentRelationship>
<ParentRelationship>
  <RelationshipName>LastModifiedBy</RelationshipName>
  <Fields>
    <string>Name</string>
  </Fields>
</ParentRelationship>
</ParentRelationships>
</Query>
<Query>
  <ObjectName>Case</ObjectName>
  <Fields>
    <string>Id</string>
    <string>IsDeleted</string>
    <string>CaseNumber</string>
    <string>SuppliedName</string>
    <string>SuppliedEmail</string>
    <string>SuppliedCompany</string>
    <string>Type</string>
    <string>Status</string>
    <string>Reason</string>
    <string>Origin</string>
    <string>Subject</string>
    <string>Description</string>
    <string>Priority</string>
    <string>IsClosed</string>
    <string>ClosedDate</string>
    <string>IsEscalated</string>
    <string>CreatedDate</string>
    <string>LastModifiedDate</string>
    <string>SystemModstamp</string>
  </Fields>
  <ParentRelationships>
    <ParentRelationship>
      <RelationshipName>Contact</RelationshipName>
    </ParentRelationship>
  </ParentRelationships>
</Query>
<string>CaseNumber</string>
<string>Subject</string>
</Fields>
</ParentRelationship>
<ParentRelationship>
<RelationshipName>CreatedBy</RelationshipName>
<Fields>
<string>Name</string>
</Fields>
</ParentRelationship>
<ParentRelationship>
<RelationshipName>LastModifiedBy</RelationshipName>
<Fields>
<string>Name</string>
</Fields>
</ParentRelationship>
</ParentRelationships>
</Query>
<Query>
<ObjectName>Contact</ObjectName>
<Fields>
<string>Id</string>
<string>IsDeleted</string>
<string>LastName</string>
<string>FirstName</string>
<string>Salutation</string>
<string>Name</string>
<string>MailingStreet</string>
<string>MailingCity</string>
<string>MailingState</string>
<string>MailingPostalCode</string>
<string>MailingCountry</string>
<string>Phone</string>
<string>Fax</string>
<string>MobilePhone</string>
<string>HomePhone</string>
<string>AssistantPhone</string>
<string>Email</string>
<string>Title</string>
<string>Department</string>
<string>AssistantName</string>
<string>LeadSource</string>
<string>Birthdate</string>
<string>Description</string>
<string>CreatedDate</string>
<string>LastModifiedDate</string>
<string>SystemModstamp</string>
<string>LastActivityDate</string>
<string>Jigsaw</string>
<string>JigsawContactId</string>
</Fields>
</Query>
<Query>
<ObjectName>MasterRecord</ObjectName>
<Fields>
<string>Name</string>
</Fields>
</Query>
<Query>
<ObjectName>Account</ObjectName>
<Fields>
<string>Name</string>
</Fields>
</Query>
<Query>
<ObjectName>ReportsTo</ObjectName>
<Fields>
<string>Name</string>
</Fields>
</Query>
</ParentRelationship>
<ParentRelationship>
    <RelationshipName>Owner</RelationshipName>
    <Fields>
        <string>Name</string>
    </Fields>
</ParentRelationship>
<ParentRelationship>
    <RelationshipName>CreatedBy</RelationshipName>
    <Fields>
        <string>Name</string>
    </Fields>
</ParentRelationship>
<ParentRelationship>
    <RelationshipName>LastModifiedBy</RelationshipName>
    <Fields>
        <string>Name</string>
    </Fields>
</ParentRelationship>
</ParentRelationships>
</Query>
<Query>
    <ObjectName>Event</ObjectName>
    <Fields>
        <string>Id</string>
        <string>Subject</string>
        <string>Location</string>
        <string>IsAllDayEvent</string>
        <string>ActivityDateTime</string>
        <string>ActivityDate</string>
        <string>DurationInMinutes</string>
        <string>StartDateTime</string>
        <string>EndDateTime</string>
        <string>Description</string>
        <string>IsPrivate</string>
        <string>ShowAs</string>
        <string>IsDeleted</string>
        <string>IsChild</string>
        <string>IsGroupEvent</string>
        <string>GroupEventType</string>
        <string>CreatedDate</string>
        <string>LastModifiedDate</string>
        <string>SystemModstamp</string>
        <string>Is Archived</string>
        <string>Is Recurrence</string>
        <string>Recurrence StartDateTime</string>
        <string>Recurrence EndDateTimeOnly</string>
        <string>Recurrence TimeZoneSidKey</string>
        <string>Recurrence Type</string>
        <string>Recurrence Interval</string>
        <string>Recurrence DayOfWeek Mask</string>
        <string>Recurrence DayOfMonth</string>
        <string>Recurrence Instance</string>
        <string>Recurrence MonthOfYear</string>
        <string>Reminder DateTime</string>
        <string>Is Reminder Set</string>
    </Fields>
    <ParentRelationships>
        <ParentRelationship>
            <RelationshipName>Who</RelationshipName>
            <Fields>
                <string>Name</string>
                <string>Type</string>
            </Fields>
        </ParentRelationship>
        <ParentRelationship>
            <RelationshipName>What</RelationshipName>
            <Fields>
                <string>Name</string>
            </Fields>
        </ParentRelationship>
    </ParentRelationships>
</Query>
<string>Type</string>
</Fields>
</ParentRelationship>
</ParentRelationship>
<RelationshipName>Account</RelationshipName>
<Fields>
<string>Name</string>
</Fields>
</ParentRelationship>
</ParentRelationship>
<RelationshipName>Owner</RelationshipName>
<Fields>
<string>Name</string>
</Fields>
</ParentRelationship>
</ParentRelationship>
<RelationshipName>CreatedBy</RelationshipName>
<Fields>
<string>Name</string>
</Fields>
</ParentRelationship>
</ParentRelationship>
<RelationshipName>LastModifiedBy</RelationshipName>
<Fields>
<string>Name</string>
</Fields>
</ParentRelationship>
</ParentRelationships>
<PolymorphicRelationships>
<PolymorphicRelationship>
<RelationshipName>Who</RelationshipName>
<ObjectName>Contact</ObjectName>
</PolymorphicRelationship>
<PolymorphicRelationship>
<RelationshipName>Who</RelationshipName>
<ObjectName>Lead</ObjectName>
</PolymorphicRelationship>
<PolymorphicRelationship>
<RelationshipName>What</RelationshipName>
<ObjectName>Account</ObjectName>
</PolymorphicRelationship>
<PolymorphicRelationship>
<RelationshipName>What</RelationshipName>
<ObjectName>Asset</ObjectName>
</PolymorphicRelationship>
<PolymorphicRelationship>
<RelationshipName>What</RelationshipName>
<ObjectName>Campaign</ObjectName>
</PolymorphicRelationship>
<PolymorphicRelationship>
<RelationshipName>What</RelationshipName>
<ObjectName>Case</ObjectName>
</PolymorphicRelationship>
<PolymorphicRelationship>
<RelationshipName>What</RelationshipName>
<ObjectName>Contract</ObjectName>
</PolymorphicRelationship>
<PolymorphicRelationship>
<RelationshipName>What</RelationshipName>
<ObjectName>Magic_Item</ObjectName>
</PolymorphicRelationship>
<PolymorphicRelationship>
<RelationshipName>What</RelationshipName>
<ObjectName>Opportunity</ObjectName>
</PolymorphicRelationship>
<PolymorphicRelationship>
<RelationshipName>What</RelationshipName>
<ObjectName>Product2</ObjectName>
</PolymorphicRelationship>
<string>RecurrenceDayOfWeekMask</string>
<string>RecurrenceDayOfMonth</string>
<string>RecurrenceInstance</string>
<string>RecurrenceMonthOfYear</string>

</Fields>
</ParentRelationships>
<ParentRelationship>
    <RelationshipName>Who</RelationshipName>
    <Fields>
        <string>Name</string>
        <string>Type</string>
    </Fields>
</ParentRelationship>
<ParentRelationship>
    <RelationshipName>What</RelationshipName>
    <Fields>
        <string>Name</string>
        <string>Type</string>
    </Fields>
</ParentRelationship>
<ParentRelationship>
    <RelationshipName>Owner</RelationshipName>
    <Fields>
        <string>Name</string>
    </Fields>
</ParentRelationship>
<ParentRelationship>
    <RelationshipName>Account</RelationshipName>
    <Fields>
        <string>Name</string>
    </Fields>
</ParentRelationship>
<ParentRelationship>
    <RelationshipName>CreatedBy</RelationshipName>
    <Fields>
        <string>Name</string>
    </Fields>
</ParentRelationship>
<ParentRelationship>
    <RelationshipName>LastModifiedBy</RelationshipName>
    <Fields>
        <string>Name</string>
    </Fields>
</ParentRelationship>
<PolymorphicRelationships>
    <PolymorphicRelationship>
        <RelationshipName>Who</RelationshipName>
        <ObjectName>Contact</ObjectName>
    </PolymorphicRelationship>
    <PolymorphicRelationship>
        <RelationshipName>Who</RelationshipName>
        <ObjectName>Lead</ObjectName>
    </PolymorphicRelationship>
    <PolymorphicRelationship>
        <RelationshipName>What</RelationshipName>
        <ObjectName>Account</ObjectName>
    </PolymorphicRelationship>
    <PolymorphicRelationship>
        <RelationshipName>What</RelationshipName>
        <ObjectName>Asset</ObjectName>
    </PolymorphicRelationship>
    <PolymorphicRelationship>
        <RelationshipName>What</RelationshipName>
        <ObjectName>Campaign</ObjectName>
    </PolymorphicRelationship>
    <PolymorphicRelationship>
        <RelationshipName>What</RelationshipName>
        <ObjectName>Case</ObjectName>
    </PolymorphicRelationship>
</PolymorphicRelationships>
<Query>
  <ObjectName>User</ObjectName>
  <Fields>
    <string>Id</string>
    <string>Username</string>
    <string>LastName</string>
    <string>FirstName</string>
    <string>Name</string>
    <string>CompanyName</string>
    <string>Division</string>
    <string>Title</string>
    <string>Street</string>
    <string>City</string>
    <string>State</string>
    <string>PostalCode</string>
    <string>Country</string>
    <string>Email</string>
    <string>Phone</string>
    <string>Fax</string>
    <string>MobilePhone</string>
    <string>Alias</string>
    <string>CommunityNickname</string>
    <string>IsActive</string>
    <string>TimeZoneSidKey</string>
    <string>LocaleSidKey</string>
    <string>ReceivesInfoEmails</string>
    <string>ReceivesAdminInfoEmails</string>
    <string>EmailEncodingKey</string>
    <string>UserType</string>
    <string>LanguageLocaleKey</string>
    <string>EmployeeNumber</string>
    <string>CreatedDate</string>
    <string>LastModifiedDate</string>
    <string>SystemModstamp</string>
    <string>UserPermissionsMarketingUser</string>
    <string>UserPermissionsOfflineUser</string>
    <string>UserPermissionsCallCenterAutoLogin</string>
    <string>UserPermissionsMobileUser</string>
    <string>UserPermissionsSFContentUser</string>
    <string>UserPermissionsKnowledgeUser</string>
    <string>UserPermissionsInteractionUser</string>
    <string>UserPermissionsSupportUser</string>
    <string>UserPermissionsSiteforceContributorUser</string>
    <string>UserPermissionsSiteforcePublisherUser</string>
    <string>UserPermissionsChatterAnswersUser</string>
  </Fields>
</Query>
<string>ForecastEnabled</string>
<string>UserPreferencesActivityRemindersPopup</string>
<string>UserPreferencesEventRemindersCheckboxDefault</string>
<string>UserPreferencesTaskRemindersCheckboxDefault</string>
<string>UserPreferencesReminderSoundOff</string>
<string>UserPreferencesDisableAllFeedsEmail</string>
<string>UserPreferencesDisableFollowersEmail</string>
<string>UserPreferencesDisableChangeCommentEmail</string>
<string>UserPreferencesDisableLaterCommentEmail</string>
<string>UserPreferencesDisProfPostCommentEmail</string>
<string>UserPreferencesContentNoEmail</string>
<string>UserPreferencesContentEmailAsAndWhen</string>
<string>UserPreferencesHideCSNGetChatterMobileTask</string>
<string>UserPreferencesDisableMentionsPostEmail</string>
<string>UserPreferencesHideCSNDesktopTask</string>
<string>UserPreferencesDisCommentAfterLikeEmail</string>
<string>UserPreferencesDisableLikeEmail</string>
<string>UserPreferencesDisableMessageEmail</string>
<string>UserPreferencesOptOutOfTouch</string>
<string>UserPreferencesDisableBookmarkEmail</string>
<string>UserPreferencesDisableSharePostEmail</string>
<string>UserPreferencesEnableAutoSubForFeeds</string>
<string>UserPreferencesDisableFileShareNotificationsForApi</string>
<string>Extension</string>
<string>FederationIdentifier</string>
<string>AboutMe</string>
<string>FullPhotoUrl</string>
<string>SmallPhotoUrl</string>
<string>DigestFrequency</string>
<string>DefaultGroupNotificationFrequency</string>
</Fields>
</ParentRelationships>
<ObjectName>Contract</ObjectName>
</PolymorphicRelationship>
<RelationshipName>Parent</RelationshipName>
<ObjectName>EmailTemplate</ObjectName>
</PolymorphicRelationship>
<RelationshipName>Parent</RelationshipName>
<ObjectName>Event</ObjectName>
</PolymorphicRelationship>
<RelationshipName>Parent</RelationshipName>
<ObjectName>Lead</ObjectName>
</PolymorphicRelationship>
<RelationshipName>Parent</RelationshipName>
<ObjectName>Magic_Item_c</ObjectName>
</PolymorphicRelationship>
<RelationshipName>Parent</RelationshipName>
<ObjectName>Opportunity</ObjectName>
</PolymorphicRelationship>
<RelationshipName>Parent</RelationshipName>
<ObjectName>Product2</ObjectName>
</PolymorphicRelationship>
<RelationshipName>Parent</RelationshipName>
<ObjectName>Solution</ObjectName>
</PolymorphicRelationship>
<RelationshipName>Parent</RelationshipName>
<ObjectName>Task</ObjectName>
</PolymorphicRelationship>
</Query>
</Query>
<ObjectName>FeedItem</ObjectName>
<Fields>
<string>Id</string>
<string>Type</string>
<string>Body</string>
<string>CreatedDate</string>
<string>IsDeleted</string>
<string>LastModifiedDate</string>
<string>SystemModstamp</string>
<string>CommentCount</string>
<string>LikeCount</string>
<string>LinkUrl</string>
<string>ContentData</string>
<string>ContentFileName</string>
<string>ContentDescription</string>
<string>ContentType</string>
<string>ContentSize</string>
</Fields>
</Query>
<ObjectName>FeedComment</ObjectName>
<Fields>
<string>Id</string>
<string>FeedItemId</string>
<string>CreatedDate</string>
<string>CommentBody</string>
<string>IsDeleted</string>
<string>CommentType</string>
<string>ParentId</string>
<string>RelatedRecordId</string>
</Fields>
</Query>
</ParentRelationships>
What's Next?

Create a mapping file for fields from obtained objects (see "Salesforce Mapping File Example for Standard Objects" on page 1507).

9.38.8.6 Salesforce ObjectsToGet Configuration File Example for Knowledge Base

Salesforce Knowledge Base content correspond to non-standard objects and fields. When your Salesforce organization contains Knowledge Base articles and you want to index their content, you must include specific queries to your custom ObjectsToGet configuration file.

The ObjectsToGet configuration file example presented in this topic specifies to retrieve two arbitrary named Knowledge Base objects:

- MyKBArticleType1
- MyKBArticleType2

**Note:** The Salesforce connector cannot index permissions of Knowledge Base articles like it can for other objects. It is therefore recommended to create a separate ObjectsToGet configuration file and source for Knowledge Base articles.

The following XML code is an ObjectsToGet configuration file example for Knowledge Base articles.

```
<ArrayOfQuery version="1.0" encoding="utf-8">
  <Query xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
        xmlns:xsd="http://www.w3.org/2001/XMLSchema">
    <ObjectName>MyKBArticleType1__ka</ObjectName>
    <Fields>
      <string>CaseAssociationCount</string>
      <string>LastModifiedDate</string>
      <string>ArticleNumber</string>
      <string>LastPublishedDate</string>
      <string>FirstPublishedDate</string>
      <string>SystemModstamp</string>
      <string>ArchivedDate</string>
      <string>CreatedDate</string>
      <string>IsDeleted</string>
    </Fields>
  </Query>
</ArrayOfQuery>
```
<string>Id</string>
</Fields>
</ParentRelationships>
<ParentRelationship>
  <RelationshipName>LastModifiedBy</RelationshipName>
  <Fields>
    <string>Name</string>
  </Fields>
</ParentRelationship>
</ParentRelationships>
</ChildRelationships>
</Query>
</Query>
<Query>
  <ObjectName>MyKBArticleType1_kav</ObjectName>
  <Fields>
    <string>ArchivedDate</string>
    <string>IsVisibleInPrm</string>
    <string>Undecipherable_Content_c</string>
    <string>IsVisibleInApp</string>
    <string>LastModifiedDate</string>
    <string>SystemModstamp</string>
    <string>IsVisibleInPkb</string>
    <string>PublishStatus</string>
    <string>IsDeleted</string>
    <string>Id</string>
    <string>IsLatestVersion</string>
    <string>CreatedDate</string>
    <string>Title</string>
    <string>LastPublishedDate</string>
    <string>Summary</string>
    <string>FirstPublishedDate</string>
    <string>ArticleNumber</string>
    <string>Language</string>
    <string>UrlName</string>
    <string>VersionNumber</string>
    <string>IsVisibleInCsp</string>
  </Fields>
  <ParentRelationships>
    <ParentRelationship>
      <RelationshipName>LastModifiedBy</RelationshipName>
      <Fields>
        <string>Name</string>
      </Fields>
    </ParentRelationship>
    <ParentRelationship>
      <RelationshipName>CreatedBy</RelationshipName>
      <Fields>
        <string>Name</string>
      </Fields>
    </ParentRelationship>
  </ParentRelationships>
</Query>
</Query>
<Query>
  <ObjectName>MyKBArticleType2_ka</ObjectName>
  <Fields>
    <string>CaseAssociationCount</string>
  </Fields>
</Query>
What's Next?

Create a mapping file for fields from obtained objects (see "Salesforce Mapping File Example for Knowledge Base" on page 1525).

9.38.8.7 Salesforce ObjectsToGet Configuration File Example for CRM Content

With Salesforce CRM Content you can organize, share, search, and manage content within your organization and across key areas of the Salesforce application. CRM Content can include all file types, from traditional business documents such as Microsoft Office documents to audio files, video files, Web pages, and Google docs (see the Salesforce document Salesforce CRM Content Overview).

When your Salesforce organization contains CRM Content and you want to index the content of these files, you must include additional queries to your custom ObjectsToGet configuration file.

The following XML code is an ObjectsToGet configuration file example for Chatter files.

```xml
<?xml version="1.0" encoding="utf-8"?>
<ArrayOfQuery xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
    xmlns:xsd="http://www.w3.org/2001/XMLSchema">
    <Query>
        <ObjectName>ContentVersion</ObjectName>
        <Fields>
            <string>CreatedDate</string>
            <string>LastModifiedDate</string>
            <string>SystemModstamp</string>
            <string>IsDeleted</string>
            <string>Id</string>
            <string>ContentDocumentId</string>
            <string>ContentModifiedById</string>
            <string>ContentModifiedDate</string>
            <string>ContentSize</string>
            <string>ContentUrl</string>
            <string>Description</string>
            <string>FeaturedContentBoost</string>
            <string>FeaturedContentDate</string>
            <string>FileType</string>
            <string>FirstPublishLocationId</string>
            <string>IsLatest</string>
            <string>NegativeRatingCount</string>
            <string>Origin</string>
            <string>OwnerId</string>
            <string>PathOnClient</string>
            <string>PositiveRatingCount</string>
            <string>PublishStatus</string>
            <string>RatingCount</string>
            <string>ReasonForChange</string>
            <string>TagCsv</string>
            <string>Title</string>
            <string>VersionData</string>
            <string>VersionNumber</string>
        </Fields>
    </Query>
</ArrayOfQuery>
```

The following XML code is an ObjectsToGet configuration file example for CRM Content.
<?xml version="1.0" encoding="utf-8"?>
<ArrayOfQuery xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns:xsd="http://www.w3.org/2001/XMLSchema">
  <Query>
    <ObjectName>ContentVersion</ObjectName>
    <Fields>
      <string>Id</string>
      <string>IsLatest</string>
      <string>ContentUrl</string>
      <string>Title</string>
      <string>IsDeleted</string>
      <string>ContentModifiedDate</string>
      <string>CreatedDate</string>
      <string>LastModifiedDate</string>
      <string>SystemModstamp</string>
      <string>PublishStatus</string>
      <string>VersionData</string>
      <string>ContentSize</string>
      <string>Origin</string>
    </Fields>
    <ParentRelationships>
      <ParentRelationship>
        <RelationshipName>ContentDocument</RelationshipName>
        <Fields>
          <string>Title</string>
        </Fields>
      </ParentRelationship>
      <ParentRelationship>
        <RelationshipName>Owner</RelationshipName>
        <Fields>
          <string>Name</string>
        </Fields>
      </ParentRelationship>
      <ParentRelationship>
        <RelationshipName>CreatedBy</RelationshipName>
        <Fields>
          <string>Name</string>
        </Fields>
      </ParentRelationship>
      <ParentRelationship>
        <RelationshipName>LastModifiedBy</RelationshipName>
        <Fields>
          <string>Name</string>
        </Fields>
      </ParentRelationship>
      <ParentRelationship>
        <RelationshipName>FirstPublishLocation</RelationshipName>
        <Fields>
          <string>Name</string><string>Type</string>
        </Fields>
      </ParentRelationship>
    </ParentRelationships>
    <PolymorphicRelationships>
      <PolymorphicRelationship>
        <RelationshipName>FirstPublishLocation</RelationshipName>
        <ObjectName>Account</ObjectName>
      </PolymorphicRelationship>
      <PolymorphicRelationship>
        <RelationshipName>FirstPublishLocation</RelationshipName>
        <ObjectName>Asset</ObjectName>
      </PolymorphicRelationship>
      <PolymorphicRelationship>
        <RelationshipName>FirstPublishLocation</RelationshipName>
        <ObjectName>Campaign</ObjectName>
      </PolymorphicRelationship>
      <PolymorphicRelationship>
        <RelationshipName>FirstPublishLocation</RelationshipName>
        <ObjectName>Case</ObjectName>
      </PolymorphicRelationship>
    </PolymorphicRelationships>
  </Query>
</ArrayOfQuery>
</PolymorphicRelationship>
PolymorphicRelationship>
<RelationshipName>FirstPublishLocation</RelationshipName>
<ObjectName>CollaborationGroup</ObjectName>
</PolymorphicRelationship>
PolymorphicRelationship>
<RelationshipName>FirstPublishLocation</RelationshipName>
<ObjectName>Contact</ObjectName>
</PolymorphicRelationship>
PolymorphicRelationship>
<RelationshipName>FirstPublishLocation</RelationshipName>
<ObjectName>ContentWorkspace</ObjectName>
</PolymorphicRelationship>
PolymorphicRelationship>
<RelationshipName>FirstPublishLocation</RelationshipName>
<ObjectName>Contract</ObjectName>
</PolymorphicRelationship>
PolymorphicRelationship>
<RelationshipName>FirstPublishLocation</RelationshipName>
<ObjectName>Dashboard</ObjectName>
</PolymorphicRelationship>
PolymorphicRelationship>
<RelationshipName>FirstPublishLocation</RelationshipName>
<ObjectName>DashboardComponent</ObjectName>
</PolymorphicRelationship>
PolymorphicRelationship>
<RelationshipName>FirstPublishLocation</RelationshipName>
<ObjectName>Event</ObjectName>
</PolymorphicRelationship>
PolymorphicRelationship>
<RelationshipName>FirstPublishLocation</RelationshipName>
<ObjectName>Lead</ObjectName>
</PolymorphicRelationship>
PolymorphicRelationship>
<RelationshipName>FirstPublishLocation</RelationshipName>
<ObjectName>Lost_Scroll_kø</ObjectName>
</PolymorphicRelationship>
PolymorphicRelationship>
<RelationshipName>FirstPublishLocation</RelationshipName>
<ObjectName>Magic_Item_c</ObjectName>
</PolymorphicRelationship>
PolymorphicRelationship>
<RelationshipName>FirstPublishLocation</RelationshipName>
<ObjectName>Magic_Spell_kø</ObjectName>
</PolymorphicRelationship>
PolymorphicRelationship>
<RelationshipName>FirstPublishLocation</RelationshipName>
<ObjectName>Opportunity</ObjectName>
</PolymorphicRelationship>
PolymorphicRelationship>
<RelationshipName>FirstPublishLocation</RelationshipName>
<ObjectName>Product2</ObjectName>
</PolymorphicRelationship>
PolymorphicRelationship>
<RelationshipName>FirstPublishLocation</RelationshipName>
<ObjectName>Report</ObjectName>
</PolymorphicRelationship>
PolymorphicRelationship>
<RelationshipName>FirstPublishLocation</RelationshipName>
<ObjectName>Site</ObjectName>
</PolymorphicRelationship>
PolymorphicRelationship>
<RelationshipName>FirstPublishLocation</RelationshipName>
<ObjectName>Solution</ObjectName>
</PolymorphicRelationship>
PolymorphicRelationship>
<RelationshipName>FirstPublishLocation</RelationshipName>
<ObjectName>Task</ObjectName>
</PolymorphicRelationship>
What's Next?

Create a mapping file for fields from obtained objects (see "Salesforce Mapping File Example for CRM Content" on page 1529).

9.38.8.8 Salesforce ObjectsToGet Configuration File Example for Chatter Objects

A variety of Salesforce objects such as User, CollaborationGroup, Account, and Case can have Chatter feeds. The list of Salesforce objects having Chatter feeds can be customized and is retrieved dynamically by the Salesforce connector. Chatter posts and comments inherit the permissions of the record onto which they are posted, no matter if that record is public, private, a group or a user. Chatter feed comments are fetched along with their parent feed item as a child relationship, they do not require additional API calls.

By default, the Salesforce connector supports the following Chatter objects and their types:

- **FeedItem** for feed item of types:
  - TextPost: a direct text entry on a feed
  - LinkPost: a URL posting on a feed
  - ContentPost: an uploaded file on a feed
  - PollPost: a poll posted on a feed

- **FeedComment** for comments on a feed item of types
  - ContentComment: an uploaded file on a comment
  - TextComment: a direct text entry on a comment

- **ContentVersion** for Chatter files
  - FeedContent: File (ContentVersion) linked to Chatter comment

**Note:** CES 7.0.8225+ (March 2016) You can link attachments to the Chatter comment in which they appear (see Modifying Hidden Salesforce Source Parameters).

You can add or remove some Chatter types (see "Indexing More Than the Built-in FeedItem Types" on page 1505) such as the following:

- **Non default FeedItem types**:
  - DashboardComponentSnapshot: a posting of a dashboard snapshot on a feed
  - TrackedChange: a change or group of changes to a tracked field
- **UserStatus**: automatically generated when a user adds a post
- **ApprovalPost**: automatically generated by a feed query on an approval item
- **CollaborationGroupCreated**: automatically generated post on a user feed when the user creates a public group
- **ActivityEvent**: generated event when a user or the API adds a task associated with a feed-enabled parent record (excluding email tasks on cases)
- **CaseCommentPost**: generated event when a user adds a case comment for a case object
- **EmailMessageEvent**: generated event when an email related to a case object is sent or received
- **CallLogPost**: generated event when a user logs a call for a case through the user interface. This event is also generated by CTI (computer-telephony integration) calls.
- **ChangeStatusPost**: generated event when a user changes the status of a case
- **AttachArticleEvent**: generated event when a user attaches an article to a case

**CollaborationGroup**

You can use metadata to link related Chatter items:

- **Any type of feed item and its comment(s)**: FeedItem.Id == FeedComment.FeedItemId

- **A feed item of type ContentPost and the corresponding uploaded Chatter file**: FeedItem.RelatedRecordId == ContentVersion.Id

- **A feed comment of type ContentComment and the corresponding uploaded Chatter file**:

  FeedComment.RelatedRecordId == ContentVersion.Id

The following code sample is the content of the ObjectsToGet configuration file example for Chatter feed for standard Service Cloud objects and fields.

```xml
    <Query>...
        <ObjectName>FeedItem</ObjectName>
        <Fields>
            <string>Id</string>
            <string>Type</string>
            <string>Body</string>
            <string>CreatedDate</string>
            <string>IsDeleted</string>
            <string>LastModifiedDate</string>
            <string>SystemModstamp</string>
            <string>CommentCount</string>
    </Query>
</ArrayOfQuery>
```

**Important:**

- **Both FeedItem and FeedComment objects** must be present in the configuration file.
- **Only Chatter feeds for objects (ex.: User, CollaborationGroup, Account...)** that are also present in the configuration file will be processed.
<Query>
<ObjectName>FeedComment</ObjectName>
<Field>
<string>Id</string>
<string>FeedItemId</string>
<string>CreatedDate</string>
<string>CommentBody</string>
<string>IsDeleted</string>
<string>CommentType</string>
<string>ParentId</string>
<string>RelatedRecordId</string>
</Field>
<ParentRelationships>
<ParentRelationship>
<RelationshipName>CreatedBy</RelationshipName>
<Field>
<string>Name</string>
<string>Type</string>
</Field>
</ParentRelationship>
<ParentRelationship>
<RelationshipName>InsertedBy</RelationshipName>
<Field>
<string>Name</string>
</Field>
</ParentRelationship>
</ParentRelationships>
<PolymorphicRelationships>
<PolymorphicRelationship>
<RelationshipName>CreatedBy</RelationshipName>
<ObjectName>User</ObjectName>
</PolymorphicRelationship>
</PolymorphicRelationships>
</Query>

<Query>
<ObjectName>ContentVersion</ObjectName>
<Field>
<string>CreatedDate</string>
<string>LastModifiedDate</string>
<string>SystemModstamp</string>
<string>IsDeleted</string>
<string>Id</string>
<string>ContentDocumentId</string>
<string>ContentModifiedById</string>
<string>ContentModifiedDate</string>
<string>ContentSize</string>
<string>ContentUrl</string>
<string>Description</string>
<string>FeaturedContentBoost</string>
<string>FeaturedContentDate</string>
<string>FileType</string>
<string>FirstPublishLocationId</string>
<string>IsLatest</string>
<string>NegativeRatingCount</string>
<string>Origin</string>
<string>OwnerId</string>
<string>PathOnClient</string>
<string>PositiveRatingCount</string>
<string>PublishStatus</string>
<string>RatingCount</string>
</Field>
</Query>
What's Next?

Create a mapping file for fields from obtained objects (see "Salesforce Mapping File Example for Chatter Objects" on page 1532).

9.38.8.9 Salesforce Connector Configuration Recipes

This topic provides Salesforce connector configuration solutions for various cases you may encounter when you want to optimize the searchability of your Salesforce content.

9.38.8.9.1 Indexing all Knowledge Base Versions and States

A Knowledge Base (KB) article has a state and a version. By default, the connector fetches the latest version of an article with the online (published) status.

**Note:** By default, the connector does not remove documents that are archived, but you can change this behavior (see "Excluding Archived Knowledge Base Articles" on page 1496).

The fields `PublishStatus` and `IsLatestVersion` respectively control which article version and state are fetched. Fetching all the versions and states means:

- Fetch the online articles
- Fetch the drafts articles
- Fetch the latest archived articles
- Fetch other archived articles

The following `ObjectsToGet` configuration file example for an article of type `Documentation` gets `Draft`, `Online`, and ` Archived` articles.

Depending on your CES version:

- **CES 7.0.7914+ (December 2015)**

  **Note:** When you choose to not index articles of a certain publish status (draft, online, archived), articles are deleted during an incremental refresh whether the `isLatestVersion` parameter value is `true` or `false`. The deletion also occurs when an article changes status.

  **Example:** You choose to only index draft articles, so when an article changes status from draft to online, the article is deleted during the next incremental refresh.
• CES 7.0.7914—(October 2015)
9.38.8.9.2 Excluding Archived Knowledge Base Articles

Note: **CES 7.0.8047+ (December 2015)** If archived KB articles are not indexed, they are automatically deleted during an incremental refresh whether the `isLatestVersion` parameter value is `true` or `false`.

**CES 7.0.7914– (October 2015)**

Archived KB articles can be removed in an incremental refresh using a destructive query as shown in the following `ObjectsToGet` configuration file example. This query will remove previously indexed documents from the index instead of adding/updating them.
Important:

- You do not need to specify fields or relationships for destructive queries. Found records will only be deleted. Keeping your ObjectsToGet short and sweet helps with debugging.
- Non-replicateable deleted objects cannot be deleted using a destructive query.

```xml
<?xml version="1.0" encoding="utf-8"?>
<ArrayOfQuery xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns:xsd="http://www.w3.org/2001/XMLSchema">
  <Query>
    <ObjectName>Documentation__ka</ObjectName>
    <Fields>
      <string>Id</string>
      <string>LastPublishedDate</string>
    </Fields>
  </Query>
  <Query>
    <ObjectName>Documentation__kav</ObjectName>
    <Fields>
      <string>Id</string>
      <string>Title</string>
    </Fields>
  </Query>
  <Query>
    <ObjectName>Documentation__kav</ObjectName>
    <FoundRecordsAreDeleted>true</FoundRecordsAreDeleted>
    <Conditions>
      <QueryCondition>
        <Field>PublishStatus</Field>
        <Operator>=</Operator>
        <Value>'Archived'</Value>
      </QueryCondition>
      <QueryCondition>
        <Field>IsLatestVersion</Field>
        <Operator>=</Operator>
        <Value>True</Value>
      </QueryCondition>
    </Conditions>
  </Query>
  <Query>
    <ObjectName>Documentation__kav</ObjectName>
    <FoundRecordsAreDeleted>true</FoundRecordsAreDeleted>
    <Conditions>
      <QueryCondition>
        <Field>PublishStatus</Field>
        <Operator>=</Operator>
        <Value>'Archived'</Value>
      </QueryCondition>
      <QueryCondition>
        <Field>IsLatestVersion</Field>
        <Operator>=</Operator>
        <Value>False</Value>
      </QueryCondition>
    </Conditions>
  </Query>
</ArrayOfQuery>
```

9.38.8.9.3 Indexing Knowledge Base Attachments

The Salesforce connector processes attachments on KB articles differently compared to normal objects (which rely on the Attachment object). Attachments on KB articles are automatically indexed when fields ending with __Name_
are specified in the ObjectsToGet configuration file such as in the following example to index the attachment of an article of type Documentation.

```xml
<?xml version="1.0" encoding="utf-8"?>
  <Query>
    <ObjectName>Documentation__ka</ObjectName>
    <Fields>
      <string>Id</string>
    </Fields>
  </Query>
  <Query>
    <ObjectName>Documentation__kav</ObjectName>
    <Fields>
      <string>Id</string>
      <string>Attachment__Name__s</string>
    </Fields>
  </Query>
</ArrayOfQuery>
```

An entry in the mapping file must also exist. As you can see below, the name of the mapping is [NameOfArticleType] Attachment:

```xml
<?xml version="1.0" encoding="Windows-1252" ?>
<SalesForce>...
  <Mapping type="Documentation Attachment">
    <ContentType>binarydata</ContentType>
  </Mapping>
...</SalesForce>
```

### 9.38.8.9.4 Fetching Records With Parent Relationships That Must Be Incrementally Updated

It is not uncommon to need to index a record with fields referring to a parent of a child relationship. The traditional way to achieve this is to use the `<ChildRelationships/>`, `<ParentRelationships/>` or `<PolymorphicRelationships/>` elements in a Query definition. However, using those element will give you records that will not be refreshed correctly. When record A references a field of the record B and record B changes, record A won’t be updated in an incremental refresh.

Let’s take a specific example, where an Opportunity is referring to an Account name. The following ObjectsToGet configuration file example produces one Opportunity record with the metadata ["Id", "Account.Name"]:

```xml
<?xml version="1.0" encoding="utf-8"?>
  <Query>
    <ObjectName>Opportunity</ObjectName>
    <Fields>
      <string>Id</string>
    </Fields>
    <ParentRelationships>
      <ParentRelationship>
        <RelationshipName>Account</RelationshipName>
        <Fields>
          <string>Name</string>
        </Fields>
      </ParentRelationship>
    </ParentRelationships>
  </Query>
</ArrayOfQuery>
```
You can solve this problem using the foreign keys. You must create two queries instead of one. The following ObjectsToGet configuration file example produces one Opportunity record with the metadata ["AccountId"] and one Account record with the metadata ["Id", "Name"].

```xml
<?xml version="1.0" encoding="utf-8"?>
  <Query>
    <ObjectName>Opportunity</ObjectName>
    <Fields>
      <string>AccountId</string>
    </Fields>
  </Query>
  <Query>
    <ObjectName>Account</ObjectName>
    <Fields>
      <string>Id</string>
      <string>Name</string>
    </Fields>
  </Query>
</ArrayOfQuery>
```

With metadata mapped to fields as follow:

- Opportunity
  - AccountId: sfaccountid
- Account
  - Id: sfaccountid
  - Name: sfaccountname

You must edit the CES [Index_Path]\Config\Config.txt file to link the two records using foreign keys as shown below:

```xml
<PhysicalIndex>
  ...
  <ForeignKeys>
    <ForeignKey ID="1">
      <KeyField>sfaccountid</KeyField>
      <ValueField>sfaccountname</ValueField>
      <FreeTextSearch>false</FreeTextSearch>
    </ForeignKey>
    ...
  </ForeignKeys>
</PhysicalIndex>
```

9.38.8.9.5 Fetching Child Relationship to Use for Folding

Fetching child relationships which are used in folding (aka: no facet) so they play well with incremental refresh is done through results folding.
Let's take a specific example, where a `Case` is referring to `CaseComments`. Similarly to the fetching parent relationship case, avoid using the `<ChildRelationships/>` element as shown below and producing one `Case` record with the metadata `"Id", "CaseComments.CommentBody"`.

```xml
<?xml version="1.0" encoding="utf-8"?>
<ArrayOfQuery xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
 xmlns:xsd="http://www.w3.org/2001/XMLSchema">
  <Query>
    <ObjectName>Case</ObjectName>
    <Fields>
      <string>Id</string>
    </Fields>
    <ChildRelationships>
      <Query>
        <ObjectName>CaseComments</ObjectName>
        <Fields>
          <string>CommentBody</string>
        </Fields>
      </Query>
    </ChildRelationships>
  </Query>
</ArrayOfQuery>
```

Rather use two or more queries:

```xml
<?xml version="1.0" encoding="utf-8"?>
<ArrayOfQuery xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
 xmlns:xsd="http://www.w3.org/2001/XMLSchema">
  <Query>
    <ObjectName>Case</ObjectName>
    <Fields>
      <string>Id</string>
    </Fields>
  </Query>
  <Query>
    <ObjectName>CaseComment</ObjectName>
    <Fields>
      <string>Id</string>
      <string>ParentId</string>
    </Fields>
  </Query>
</ArrayOfQuery>
```

Now all that is left to do is to use the user interface folding component to fold `CaseComments` under `Case` documents like in the Coveo JavaScript Search (see Folding Component).

### 9.38.8.9.6 Fetch Child Relationship to Use to Increase or Reduce Results From Queries

Fetching child relationships which are used to increase or reduce the number of results (aka: no facet) so they play well with incremental refresh is done through nested queries.

Like in other cases, avoid using the `<ChildRelationships/>` element and rather use two or more queries. You can use the example from the previous recipe for the ObjectsToGet configuration file.

You can then use the nested query in the query parameters or the query extension language of the user interface.

A simple, but real use case is to query the `Cases` AND `CaseComments` documents but only return `Cases` as follows:

```text
@sfid=[[@syssfcaseid] @objecttype=CaseComment q] // Where q is the keyword.
```
9.38.8.9.7 Minimizing API Calls and Object Description Prefetching

By default, the connector prefetches the descriptions of every object in the Salesforce organization to minimize the number of API calls used based on the following assumptions:

- Fetching an object costs 1 API call.
- Prefetching 200 objects costs 1 API call.
- An organization typically has 500-1000 objects.
- An ObjectsToGet configuration file typically queries 10-20 objects.

**Example:** An organization has 1000 objects and the source query in the ObjectsToGet configuration file includes 20 objects. An incremental refresh is scheduled every 5 minutes, so 24 h / 5 min = 288 refreshes per day.

- **Without prefetching:** 20 obj. * 288 incr. refr. = 5760 calls per day.
- **With prefetching:** (1000 obj. / 200 obj. per prefetch) * 288 incr. refr. = 1440 calls per day.

Using prefetching consumes four times less calls in this case.

Prefetching object descriptions does not always minimize API calls.

**Example:** An organization has 2000 objects and the source query in the ObjectsToGet configuration file includes 5 objects. An incremental refresh is scheduled every 5 minutes, so 24 h / 5 min = 288 refreshes per day.

- **Without prefetching:** 5 obj. * 288 incr. refr. = 1440 calls per day.
- **With prefetching:** (2000 obj. / 200 obj. per prefetch) * 288 incr. refr. = 2880 calls per day.

In this scenario, turning off prefetching is beneficial.

You can turn prefetching off by setting the hidden Salesforce source parameter PrefetchObjectDescriptions to False (see "PrefetchObjectDescriptions (Boolean)" on page 1545). The formula to determine the optimal value for the PrefetchObjectDescriptions parameter is:

\[
\text{PrefetchObjectDescriptions} = \frac{\text{ObjectsToGet.Objects.Count}}{\text{Organization.Objects.Count}} > 200
\]

9.38.8.9.8 Fetching Records Faster Using the Turbo Mode Runner

The connector default behavior when fetching records of a query is:

1. Make an API call to get page 1, and then wait for the records.
2. Process the records.
3. Make an API call to get page 2, and so on.

For some queries, this process can take days. The alternative solution in such cases is to use the TurboMode runner.
When to use

Consider using the TurboMode runner when:

- The query generally takes a long time to execute.
- An investigation showed that Salesforce returns small pages of results (ex: 1-5 items per page).
- An investigation showed that Salesforce takes a long time to generate a page (ex: 1-3 seconds per page).
- The following disadvantages are acceptable:
  - More API calls are needed.
  - More free memory is needed.
  - Does not work for queries with an IN condition on Id.
  - Fetched items are not sorted (so pausing/resuming the connector on that query will refetch all the items).

**Important:** A Salesforce source using the TurboMode runner for one of its queries must have its own dedicated credentials to prevent errors for other sources running in parallel.

How to use

You can activate the TurboMode runner in the ObjectsToGet configuration file as follows:

```xml
<Query>
  <Runner>TurboMode</Runner>
  ...
</Query>
```

How it works

With the Turbo Mode query runner, the Salesforce connector executes two query types in parallel:

- **Id fetcher**
  
  One query asynchronously fetches all the ids of the records and puts them in a queue. This query is executed by 1 thread and is fast, regardless of the real query to execute.

- **Record fetchers**
  
  Several queries representing the real query to execute, take up to 200 ids each, fetch the records, and put them in another queue. These queries are slow, but are executed in parallel by N threads. In practice, N = 8, limited by a hard limit from Salesforce (see Query Locator).

The query runner coordinates the threads and serves the fetched records to the caller as a simple only-read-once IEnumerable.
Example: The following query applies to 100,000 records.

```
SELECT Id, Subject, (SELECT Email FROM Shares) FROM Account
```

With the default runner, if Salesforce sends pages of 5 records every 3 seconds, it will take more than 16 hours to fetch all the records.

With the TurboMode runner, the Id fetcher query is:

```
SELECT Id FROM Account
```

and the Record fetcher queries are:

```
SELECT Id, Subject, (SELECT Email FROM Shares) FROM Account WHERE Id IN (...)
```

Note: Between fetching IDs and fetching records, records can be deleted in Salesforce. In this case, the IDs are simply ignored by Salesforce.

9.38.8.9.9 Reducing the Metadata Package Size by Scoping Parents of ContentVersion and Attachment Objects

ContentVersion and Attachment objects look up their parent objects to resolve record permissions. The default behavior of the connector is to fetch the metadata package for all parents of those objects to determine their sharing models. For some Salesforce organizations, the fetched metadata package can become too big.

You can specify a special InCondition on the field ParentObjectType in the ObjectsToGet configuration file to scope the parents of a record to specific values and consequently, reduce the size of the metadata package to fetch.

Important: With this technique, permissions on records are not fully indexed. Only parent records of specified parent objects are considered to determine the permissions of records.

Example: With the following query, the ContentVersion record permissions are the aggregation of parent Case and Opportunity records.

```
(Query)
  <ObjectName>ContentVersion</ObjectName>
  <Fields>
    <string>Id</string>
  </Fields>
  <Conditions>
    <InCondition>
      <Field>ParentObjectType</Field>
      <AllowedValues>
        <SoqlString>Case</SoqlString>
        <SoqlString>Opportunity</SoqlString>
      </AllowedValues>
    </InCondition>
  </Conditions>
</Query>
```

9.38.8.9.10 Choosing the Optimal Record Modification Date Field

When indexing records, you can select from multiple fields such as the following to set the record modification date:
• **SystemModstamp**: Updated when a user or a script modifies the record.

• **LastModifiedDate**: Updated when a user modifies the record.

• **CreatedDate**: Set when the record is created.

The preferred field is **SystemModstamp** because it is updated more often.

**Example:** In a frequent scenario where a Case is assigned to a user or a queue due to assignment rules, the OwnerId field is modified by an internal script. The SystemModstamp field is modified but not LastModifiedDate and CreatedDate.

### 9.38.8.9.11 Removing Leading Zeros of a Field

When a field is an Auto Number, the connector produces an extra metadata with the suffix `__stripped` that contains the value without the leading zeros. You can use this field when you want to show or use the values without the leading zeroes.

**Example:**

<table>
<thead>
<tr>
<th>MyField_c: 0000123</th>
</tr>
</thead>
<tbody>
<tr>
<td>MyField_c__stripped: 123</td>
</tr>
</tbody>
</table>

### 9.38.8.9.12 Using the Currency Field Converter

The connector is able to interpret currencies. When the user crawling the source is configured with a **Single Currency** mode, extra metadata is generated for records.

When a field is a currency, its value is converted to the user currency and a new metadata is created with the suffix `_converted`.

### 9.38.8.9.13 Using the FiscalYearResolver

When a field is a date and has a value, the fiscal year resolver creates additional metadata on the records with the following suffixes:

`__fiscal_year`
`__fiscal_quarter`
`__fiscal_month`
`__fiscal_week`
`__fiscal_pretty_quarter`

You can turn off the creation of these extra metadata by setting the LoadFiscalYearMetadata hidden source parameter to False (see "LoadFiscalYearMetadata (Boolean)" on page 1543).

### 9.38.8.9.14 Fixing the Feed Tracking Error

You can get a typical Salesforce source error that looks like:

Error with ID 'SALESFORCE_INVALID_QUERY': Cannot find child relationship 'Feeds' on object 'Products/Licenses' ('Case'). Make sure 'Feed Tracking' is enabled for this object in Salesforce.
When indexing Chatter items, the connector checks the parent related to field on all Chatter objects to differentiate a Chatter object from a normal object. Some objects do not have the child relationship 'Feeds' because the feed tracking is disable. This relationship is how the connector obtains related Chatter object.

You can resolve this error type by activating feed tracking (see Customizing Chatter Feed Tracking).

9.38.8.9.15 Indexing More Than the Built-in FeedItem Types

By default, the connector indexes the following Chatter feed types: TextPost, LinkPost, ContentPost, and PollPost.

In the ObjectsToGet configuration file, you can override this behavior using an InCondition in the query definition of FeedItem.

Example: The following ObjectsToGet configuration file query indexes only FeedItem of types TextPost and TrackedChanged.

```xml
<Query>
  <ObjectName>FeedItem</ObjectName>
  <Fields>
    <string>Id</string>
  </Fields>
  <Conditions>
    <InCondition>
      <Field>Type</Field>
      <AllowedValues>
        <SoqlString>TextPost</SoqlString>
        <SoqlString>TrackedChange</SoqlString>
      </AllowedValues>
    </InCondition>
  </Conditions>
</Query>
```

9.38.9 Creating a Salesforce Mapping File

The Coveo Salesforce connector can optionally use a mapping file to determine how to transfer values retrieved from Salesforce object fields to Coveo document fields.

By default, when no mapping file is referenced in a source, the connector creates a Coveo document field for each Salesforce object field using the same name.

A Salesforce mapping file specifies:

- Salesforce objects, fields, and binary data to index.
- The body of the indexed documents.
- Item relationships

You may want to create a mapping file and link it to a source when you want to:

- Control which Salesforce object fields are indexed. Only those mapped are indexed.
- Group two or more Salesforce object field to create one Coveo field.
- Add a prefix such as sf to Coveo fields for example to distinguish them from fields with the same name from
other types of sources.

- Define a custom **body** for one or more objects to control what appears in search result excerpt and Quick View for these objects.
- Manage custom elements.

It is recommended to create separate mapping files with separate sources for the following types of Salesforce content:

- Service Cloud standard and custom objects and fields
- Knowledge base articles
- CRM Content
- Chatter

**To create a Salesforce mapping file**

1. Refer to the most appropriate of the following topics to copy the content of the corresponding XML mapping file to start with a set of mappings:
   - “Salesforce Mapping File Example for Standard Objects” on page 1507
   - “Salesforce Mapping File Example for Knowledge Base” on page 1525
   - “Salesforce Mapping File Example for CRM Content” on page 1529
   - “Salesforce Mapping File Example for Chatter Objects” on page 1532

2. Using a text editor:
   a. Paste the content of the copied mapping file.
   b. When applicable to your Salesforce organization:
      - Modify or remove mappings for standard objects and fields.
      - Add mappings for custom objects and fields.

   **Note:** CES comes with built-in Salesforce Legacy connector fields where field names are prefixed with `sysssf` (see API Reference `sysssf fields`). You can reuse these fields with this second generation Salesforce connector to be able to use the out-of-the-box Coveo .NET Front-End CRM search interface.
   c. Save your mapping file.

3. Using an administrator account, connect to the Coveo Master server, and copy your custom mapping file to a location accessible to CES.

   **Example:** On the Coveo Master server, save the mapping file for Knowledge Base articles as: `D:\CES7\Config\Salesforce_KB_mapping.xml`. 
You will specify the full path to this file when you configure your Salesforce source (see "Mapping File" on page 1540).

What's Next?

Configure an Email security provider needed by the Salesforce security provider (see "Configuring an Email Security Provider" on page 65).

9.38.9.1 Salesforce Mapping File Example for Standard Objects

The basic mapping file example presented in this topic includes mappings for Salesforce Service Cloud standard objects and fields that can be useful to index. This example is a good starting point to create a new Salesforce mapping file.

The example contains mapping for the following Service Cloud standard objects:

- Binary data
- Account
- Case
- Case comment
- Contact
- Event
- Solution
- Task
- User
- Attachment

```xml
<?xml version="1.0" encoding="UTF-8"?>
<Mappings>
  <Version>1</Version>
  <CommonMapping>
    <Title>%[title]</Title>
    <Fields>
      <Field name="sourcetype">Salesforce</Field>
      <Field name="SfOrganizationId">%coveo_organization_id</Field>
      <Field name="sysauthor">%Owner.Name</Field>
      <Field name="sysdate">%SystemModstamp</Field>
      <Field name="sysSfId">%Id</Field>
      <Field name="SfId">%Id</Field>
      <Field name="SfName">%Name</Field>
      <Field name="SfCreatedDate">%CreatedDate</Field>
      <Field name="SfCreatedByName">%CreatedBy.Name</Field>
      <Field name="SfCreatedById">%CreatedBy.Id</Field>
      <Field name="SfIsDeleted">%IsDeleted</Field>
      <Field name="SfParticipantId">%Contact.Id; %Owner.Id; %LastModifiedBy.Id; %Contact.Name</Field>
      <Field name="SfParticipantName">%CreatedBy.Name; %Owner.Name; %LastModifiedBy.Name; %Contact.Name</Field>
    </Fields>
  </CommonMapping>
</Mappings>
```
<Mapping type="Account">
  <Title>%[Name]</Title>
  <Body>%[Description]</Body>
  <Fields>
    <Field name="objecttype">Account</Field>
    <Field name="objecttypename">Account</Field>
    <Field name="sfinterfaceid">service</Field>
    <Field name="SfAccountId">%[Id]</Field>
    <Field name="SfAccountName">%[Name]</Field>
    <Field name="SfAccountCustomerType">%[Type]</Field>
    <Field name="SfAccountOwnership">%[Ownership]</Field>
    <Field name="SfAccountPhone">%[Phone]</Field>
    <Field name="SfAccountRating">%[Rating]</Field>
    <Field name="SfAccountSic">%[Sic]</Field>
    <Field name="SfAccountSource">%[AccountSource]</Field>
    <Field name="SfAccountId">%[Id]</Field>
    <Field name="SfAccountNumber">%[AccountNumber]</Field>
    <Field name="SfAccountNumberOfEmployees">%[NumberOfEmployees]</Field>
    <Field name="SfAccountOwnership">%[Ownership]</Field>
    <Field name="SfAccountPhone">%[Phone]</Field>
    <Field name="SfAccountRating">%[Rating]</Field>
    <Field name="SfAccountSic">%[Sic]</Field>
    <Field name="SfAccountSource">%[AccountSource]</Field>
    <Field name="SfAccountWebsite">%[Website]</Field>
    <Field name="SfAccountType">%[Type]</Field>
    <Field name="SfAccountWebsite">%[Website]</Field>
    <Field name="SfCity">%[BillingCity]</Field>
    <Field name="SfCountry">%[BillingCountry]</Field>
    <Field name="SfFax">%[Fax]</Field>
    <Field name="SfIndustry">%[Industry]</Field>
    <Field name="SfJigsaw">%[Jigsaw]</Field>
    <Field name="SfJigsawCompanyId">%[JigsawCompanyId]</Field>
    <Field name="SfLastActivityDate">%[LastActivityDate]</Field>
    <Field name="SfLastActivityDate">%[LastActivityDate]</Field>
    <Field name="SfLastActivityDatefq">%[LastActivityDate_fiscalquarter]</Field>
    <Field name="SfLastActivityDatefy">%[LastActivityDate_fiscalyear]</Field>
    <Field name="SfLastModifiedById">%[LastModifiedBy.Id]</Field>
    <Field name="SfLastModifiedByName">%[LastModifiedBy.Name]</Field>
    <Field name="SfLastModifiedDate">%[LastModifiedDate]</Field>
    <Field name="SfLastModifiedDatefq">%[LastModifiedDate_fiscalquarter]</Field>
    <Field name="SfLastModifiedDatefy">%[LastModifiedDate_fiscalyear]</Field>
    <Field name="SfMasterRecordId">%[MasterRecord.Id]</Field>
    <Field name="SfMasterRecordName">%[MasterRecord.Name]</Field>
    <Field name="SfOwnerId">%[Owner.Id]</Field>
    <Field name="SfOwnerName">%[Owner.Name]</Field>
    <Field name="SfParentId">%[Parent.Id]</Field>
    <Field name="SfParentName">%[Parent.Name]</Field>
    <Field name="SfPostalCode">%[BillingPostalCode]</Field>
    <Field name="SfState">%[BillingState]</Field>
    <Field name="SfStreet">%[BillingStreet]</Field>
    <Field name="SfSystemModstamp">%[SystemModstamp]</Field>
    <Field name="SfJigsawCompanyId">%[JigsawCompanyId]</Field>
    <Field name="SfJigsaw">%[Jigsaw]</Field>
    <Field name="SfLastActivityDate">%[LastActivityDate]</Field>
  </Fields>
</Mapping>

<Mapping type="Account">
  <Title>%[Name]</Title>
  <Body>%[Description]</Body>
  <Fields>
    <Field name="objecttype">Case</Field>
    <Field name="objecttypename">Case</Field>
    <Field name="sfinterfaceid">service</Field>
    <Field name="SfAccountId">%[Id]</Field>
    <Field name="SfAccountName">%[Name]</Field>
    <Field name="SfAssetId">%[Asset.Id]</Field>
    <Field name="SfAssetName">%[Asset.Name]</Field>
    <Field name="SfCaseClosedDate">%[ClosedDate]</Field>
    <Field name="SfCaseClosedDatefq">%[ClosedDate_fiscalquarter]</Field>
    <Field name="SfCaseClosedDatefy">%[ClosedDate_fiscalyear]</Field>
    <Field name="SfCaseDescription">%[Description]</Field>
    <Field name="SfCaseId">%[Id]</Field>
    <Field name="SfCaseNumber">%[CaseNumber]</Field>
    <Field name="SfCaseOwner">%[CaseOwner]</Field>
    <Field name="SfCaseStatus">%[Status]</Field>
    <Field name="SfCreatedById">%[CreatedById]</Field>
    <Field name="SfCreator">%[Creator]</Field>
    <Field name="SfCreatedDate">%[CreatedDate]</Field>
    <Field name="SfSystemModstamp">%[SystemModstamp]</Field>
    <Field name="SfJigsaw">%[Jigsaw]</Field>
    <Field name="SfJigsawCompanyId">%[JigsawCompanyId]</Field>
    <Field name="SfSfCaseId">%[SfCaseId]</Field>
    <Field name="SfSfCaseNumber">%[SfCaseNumber]</Field>
    <Field name="SfSfOwnerId">%[SfOwnerId]</Field>
    <Field name="SfSfOwnerType">%[SfOwnerType]</Field>
    <Field name="SfSfOwnerId">%[SfOwnerId]</Field>
    <Field name="SfSfOwnerName">%[SfOwnerName]</Field>
    <Field name="SfSfParentId">%[SfParentId]</Field>
    <Field name="SfSfParentName">%[SfParentName]</Field>
    <Field name="SfSfPostalCode">%[SfPostalCode]</Field>
    <Field name="SfSfState">%[SfState]</Field>
    <Field name="SfSfStreet">%[SfStreet]</Field>
    <Field name="SfSfSystemModstamp">%[SfSystemModstamp]</Field>
  </Fields>
</Mapping>
<Fields>
  <Field name="SfBirthdate">%[Birthdate]</Field>
  <Field name="SfBirthdatefq">%[birthdate_fiscalquarter]</Field>
  <Field name="SfBirthdatefy">%[birthdate_fiscalyear]</Field>
  <Field name="SfCity">%[MailingCity]</Field>
  <Field name="SfContactAssistantName">%[AssistantName]</Field>
  <Field name="SfContactAssistantPhone">%[AssistantPhone]</Field>
  <Field name="SfContactDepartment">%[Department]</Field>
  <Field name="SfContactDescription">%[Description]</Field>
  <Field name="SfContactFirstName">%[FirstName]</Field>
  <Field name="SfContactId">%[Id]</Field>
  <Field name="SfContactLastName">%[LastName]</Field>
  <Field name="SfContactPhone">%[Phone]</Field>
  <Field name="SfContactSalutation">%[Salutation]</Field>
  <Field name="SfContactTitle">%[Title]</Field>
  <Field name="SfCountry">%[MailingCountry]</Field>
  <Field name="SfEmail">%[Email]</Field>
  <Field name="SfEmailDomainName">%[Email_DomainName]</Field>
  <Field name="SfEmailFullDomainName">%[Email_FullDomainName]</Field>
  <Field name="SfFax">%[Fax]</Field>
  <Field name="SfHomePhone">%[HomePhone]</Field>
  <Field name="SfJigsaw">%[Jigsaw]</Field>
  <Field name="SfJigsawContactId">%[JigsawContactId]</Field>
  <Field name="SfLastActivityDate">%[LastActivityDate]</Field>
  <Field name="SfLastActivityDatefq">%[LastActivityDate_fiscalquarter]</Field>
  <Field name="SfLastActivityDatefy">%[LastActivityDate_fiscalyear]</Field>
  <Field name="SfLastModifiedById">%[LastModifiedBy.Id]</Field>
  <Field name="SfLastModifiedByName">%[LastModifiedBy.Name]</Field>
  <Field name="SfLastModifiedDate">%[LastModifiedDate]</Field>
  <Field name="SfLastModifiedDatefq">%[LastModifiedDate_fiscalquarter]</Field>
  <Field name="SfLastModifiedDatefy">%[LastModifiedDate_fiscalyear]</Field>
  <Field name="SfLeadSource">%[LeadSource]</Field>
  <Field name="SfMasterRecordId">%[MasterRecord.Id]</Field>
  <Field name="SfMasterRecordName">%[MasterRecord.Name]</Field>
  <Field name="SfMobilePhone">%[MobilePhone]</Field>
  <Field name="SfOwnerId">%[Owner.Id]</Field>
  <Field name="SfOwnerName">%[Owner.Name]</Field>
  <Field name="SfPostalCode">%[MailingPostalCode]</Field>
  <Field name="SfReportsToId">%[ReportsTo.Id]</Field>
  <Field name="SfReportsToName">%[ReportsTo.Name]</Field>
  <Field name="SfState">%[MailingState]</Field>
  <Field name="SfStreet">%[MailingStreet]</Field>
  <Field name="SfSystemModstamp">%[SystemModstamp]</Field>
  <Field name="SfSystemModstampfq">%[SystemModstamp_fiscalquarter]</Field>
  <Field name="SfSystemModstampfy">%[SystemModstamp_fiscalyear]</Field>
</Fields>
</Mapping>
<Mapping type="Event">
  <Title>%%[Subject]</Title>
  <Body>%%[Subject]</Body>
  <Fields>
    <Field name="objecttype">Event</Field>
    <Field name="objecttypename">Event</Field>
    <Field name="sfinterfaceid">service</Field>
    <Field name="SfAccountId">%[Account.Id]</Field>
    <Field name="SfAccountName">%[Account.Name]</Field>
    <Field name="SfActivityDate">%[ActivityDate]</Field>
    <Field name="SfActivityDatefq">%[ActivityDate_fiscalquarter]</Field>
    <Field name="SfActivityDatefy">%[ActivityDate_fiscalyear]</Field>
    <Field name="SfAssetId">%[What_Asset.Id]</Field>
    <Field name="SfAssetName">%[What_Asset.Name]</Field>
    <Field name="SfCampaignId">%[What_Campaign.Id]</Field>
    <Field name="SfCampaignName">%[What_Campaign.Name]</Field>
    <Field name="SfCaseId">%[What_Case.Id]</Field>
    <Field name="SfCaseName">%[What_Case.Name]</Field>
    <Field name="SfContactId">%[Who_Contact.Id]</Field>
    <Field name="SfContactName">%[Who_Contact.Name]</Field>
    <Field name="SfContractId">%[What_Contract.Id]</Field>
  </Fields>
</Mapping>
<Field name="SFContractName">% [What_Contract_Name]</Field>
<Field name="SFEventActivityDateTime">% [ActivityDateTime]</Field>
<Field name="SFEventActivityDateTimef">% [ActivityDateTime_fiscalquarter]</Field>
<Field name="SFEventActivityDateTimefy">% [ActivityDateTime_fiscalyear]</Field>
<Field name="SFEventDescription">% [Description]</Field>
<Field name="SFEventDurationInMinutes">% [DurationInMinutes]</Field>
<Field name="SFEventEndDate">% [EndDateTime]</Field>
<Field name="SFEventEndDatef">% [EndDateTime_fiscalquarter]</Field>
<Field name="SFEventEndDateTimefy">% [EndDateTime_fiscalyear]</Field>
<Field name="SFEventGroupEventType">% [GroupEventType]</Field>
<Field name="SFEventId">% [Id]</Field>
<Field name="SFEventIsAllDayEvent">% [IsAllDayEvent]</Field>
<Field name="SFEventIsChild">% [IsChild]</Field>
<Field name="SFEventIsGroupEvent">% [IsGroupEvent]</Field>
<Field name="SFEventReminderDateTime">% [ReminderDateTime]</Field>
<Field name="SFEventReminderDateTimef">% [ReminderDateTime_fiscalquarter]</Field>
<Field name="SFEventReminderDateTimefy">% [ReminderDateTime_fiscalyear]</Field>
<Field name="SFEventShowAs">% [ShowAs]</Field>
<Field name="SFIsArchived">% [IsArchived]</Field>
<Field name="SFIsPrivate">% [IsPrivate]</Field>
<Field name="SFIsRecurrence">% [IsRecurrence]</Field>
<Field name="SFIsReminderSet">% [IsReminderSet]</Field>
<Field name="SFLastModifiedById">% [LastModifiedById]</Field>
<Field name="SFLastModifiedByName">% [LastModifiedBy_Name]</Field>
<Field name="SFLastModifiedDate">% [LastModifiedDate]</Field>
<Field name="SFLastModifiedDatef">% [LastModifiedDate_fiscalquarter]</Field>
<Field name="SFLastModifiedDatefy">% [LastModifiedDate_fiscalyear]</Field>
<Field name="SFLocation">% [Location]</Field>
<Field name="SFMagic_Item_cId">% [What_Magic_Item_c.Id]</Field>
<Field name="SFMagic_Item_cName">% [What_Magic_Item_c.Name]</Field>
<Field name="SFOpportunityId">% [What_Opportunity.Id]</Field>
<Field name="SFOpportunityName">% [What_Opportunity.Name]</Field>
<Field name="SFOwnerId">% [Owner.Id]</Field>
<Field name="SFOwnerName">% [Owner.Name]</Field>
<Field name="SFProduct2Id">% [What_Product2.Id]</Field>
<Field name="SFProduct2Name">% [What_Product2.Name]</Field>
<Field name="SFRecurrenceDayOfMonth">% [RecurrenceDayOfMonth]</Field>
<Field name="SFRecurrenceDayOfWeekMask">% [RecurrenceDayOfWeekMask]</Field>
<Field name="SFRecurrenceEndDateTimeOnly">% [RecurrenceEndDateTimeOnly]</Field>
<Field name="SFRecurrenceEndDateTimeOnlyf">% [RecurrenceEndDateTimeOnly_fiscalquarter]</Field>
<Field name="SFRecurrenceEndDateTimeOnlyfy">% [RecurrenceEndDateTimeOnly_fiscalyear]</Field>
<Field name="SFRecurrenceInstance">% [RecurrenceInstance]</Field>
<Field name="SFRecurrenceInterval">% [RecurrenceInterval]</Field>
<Field name="SFRecurrenceMonthOfYear">% [RecurrenceMonthOfYear]</Field>
<Field name="SFRecurrenceStartDateTime">% [RecurrenceStartDateTime]</Field>
<Field name="SFRecurrenceStartDateTimef">% [RecurrenceStartDateTime_fiscalquarter]</Field>
<Field name="SFRecurrenceStartDateTimefy">% [RecurrenceStartDateTime_fiscalyear]</Field>
<Field name="SFRecurrenceTimeZoneSidKey">% [RecurrenceTimeZoneSidKey]</Field>
<Field name="SFRecurrenceType">% [RecurrenceType]</Field>
<Field name="SFSolutionId">% [What_Solution.Id]</Field>
<Field name="SFSolutionName">% [What_Solution.Name]</Field>
<Field name="SFSystemModstamp">% [SystemModstamp]</Field>
<Field name="SFSystemModstampf">% [SystemModstamp_fiscalquarter]</Field>
<Field name="SFSystemModstampfy">% [SystemModstamp_fiscalyear]</Field>
<Field name="SFWhatId">% [What.Id]</Field>
<Field name="SFWhatName">% [What.Name]</Field>
<Field name="SFWhoId">% [Who.Id]</Field>
<Field name="SFWhoName">% [Who.Name]</Field>
<Field name="sysfiletype">SalesforceItem</Field>
</Fields>
</Mapping>
<Mapping type="Solution">
  <Title>% [SolutionName] / Title</Title>
<Body>%[SolutionNote]</Body>

<Field name="objecttype">Solution</Field>
<Field name="objecttypename">Solution</Field>
<Field name="sfinterfaceid">service</Field>
<Field name="SfIsHtml">%[IsHtml]</Field>
<Field name="SfIsPublished">%[IsPublished]</Field>
<Field name="SfLastModifiedById">%[LastModifiedBy.Id]</Field>
<Field name="SfLastModifiedByName">%[LastModifiedBy.Name]</Field>
<Field name="SfLastModifiedDate">%[LastModifiedDate]</Field>
<Field name="SfLastModifiedDatefq">%[LastModifiedDate_fiscalquarter]</Field>
<Field name="SfLastModifiedDatefy">%[LastModifiedDate_fiscalyear]</Field>
<Field name="SfOwnerId">%[Owner.Id]</Field>
<Field name="SfOwnerName">%[Owner.Name]</Field>
<Field name="SfSolutionId">%[Id]</Field>
<Field name="SfSolutionIsPublishedInPublicKb">%[IsPublishedInPublicKb]</Field>
<Field name="SfSolutionIsReviewed">%[IsReviewed]</Field>
<Field name="SfSolutionName">%[SolutionName]</Field>
<Field name="SfSolutionNote">%[SolutionNote]</Field>
<Field name="SfSolutionSolutionNumber">%[SolutionNumber]</Field>
<Field name="SfSolutionStatus">%[Status]</Field>
<Field name="SfSolutionTimesUsed">%[TimesUsed]</Field>
<Field name="SfSystemModstamp">%[SystemModstamp]</Field>
<Field name="SfSystemModstampfq">%[SystemModstamp_fiscalquarter]</Field>
<Field name="SfSystemModstampfy">%[SystemModstamp_fiscalyear]</Field>
<Field name="sysfiletype">SalesforceItem</Field>
<Field name="SfRecurrenceDayOfMonth">%{RecurrenceDayOfMonth}</Field>
<Field name="SfRecurrenceDayOfWeekMask">%{RecurrenceDayOfWeekMask}</Field>
<Field name="SfRecurrenceEndDateOnly">%{RecurrenceEndDateOnly}</Field>
<Field name="SfRecurrenceEndDateOnlyfq">%{RecurrenceEndDateOnly_fiscalquarter}</Field>
<Field name="SfRecurrenceEndDateOnlyfy">%{RecurrenceEndDateOnly_fiscalyear}</Field>
<Field name="SfRecurrenceInstance">%{RecurrenceInstance}</Field>
<Field name="SfRecurrenceInterval">%{RecurrenceInterval}</Field>
<Field name="SfRecurrenceMonthOfYear">%{RecurrenceMonthOfYear}</Field>
<Field name="SfRecurrenceStartDateOnly">%{RecurrenceStartDateOnly}</Field>
<Field name="SfRecurrenceStartDateOnlyfq">%{RecurrenceStartDateOnly_fiscalquarter}</Field>
<Field name="SfRecurrenceStartDateOnlyfy">%{RecurrenceStartDateOnly_fiscalyear}</Field>
<Field name="SfRecurrenceTimeZoneSidKey">%{RecurrenceTimeZoneSidKey}</Field>
<Field name="SfRecurrenceType">%{RecurrenceType}</Field>
<Field name="SfSolutionId">%{What_Solution.Id}</Field>
<Field name="SfSolutionName">%{What_Solution.Name}</Field>
<Field name="SfSystemModstamp">%{SystemModstamp}</Field>
<Field name="SfSystemModstampfq">%{SystemModstamp_fiscalquarter}</Field>
<Field name="SfSystemModstampfy">%{SystemModstamp_fiscalyear}</Field>
<Field name="SfTaskCallDisposition">%{CallDisposition}</Field>
<Field name="SfTaskCallType">%{CallType}</Field>
<Field name="SfTaskDescription">%{Description}</Field>
<Field name="SfTaskId">%{Id}</Field>
<Field name="SfTaskPriority">%{Priority}</Field>
<Field name="SfTaskStatus">%{Status}</Field>
<Field name="SfTaskSubject">%{Subject}</Field>
<Field name="SfWhatId">%{What.Id}</Field>
<Field name="SfWhatName">%{What.Name}</Field>
<Field name="SfWhoId">%{Who.Id}</Field>
<Field name="SfWhoName">%{Who.Name}</Field>
<Field name="sysfiletype">SalesforceItem</Field>
<html>
</html>
<Field name="SfUserCommunityNickname">%CommunityNickname</Field>
<Field name="SfUserCompanyName">%CompanyName</Field>
<Field name="SfUserDefaultGroupNotificationFrequency">%DefaultGroupNotificationFrequency</Field>
<Field name="SfUserDepartment">%Department</Field>
<Field name="SfUserDigestFrequency">%DigestFrequency</Field>
<Field name="SfUserDivision">%Division</Field>
<Field name="SfUserEmailEncodingKey">%EmailEncodingKey</Field>
<Field name="SfUserEmployeeNumber">%EmployeeNumber</Field>
<Field name="SfUserExtension">%Extension</Field>
<Field name="SfUserFederationIdentifier">%FederationIdentifier</Field>
<Field name="SfUserFirstName">%FirstName</Field>
<Field name="SfUserForecastEnabled">%ForecastEnabled</Field>
<Field name="SfUserID">%Id</Field>
<Field name="SfUserLastName">%LastName</Field>
<Field name="SfUserLocaleSidKey">%LocaleSidKey</Field>
<Field name="SfUserName">%Name</Field>
<Field name="SfUserPhone">%Phone</Field>
<Field name="SfUserReceivesAdminInfoEmails">%ReceivesAdminInfoEmails</Field>
<Field name="SfUserReceivesInfoEmails">%ReceivesInfoEmails</Field>
<Field name="SfUserRole.Id">%UserRole.Id</Field>
<Field name="SfUserRole.Name">%UserRole.Name</Field>
<Field name="SfUserTimezoneSidKey">%TimezoneSidKey</Field>
<Field name="SfUserTitle">%Title</Field>
<Field name="SfUserUserPermissionsCallCenterAutoLogin">%UserPermissionsCallCenterAutoLogin</Field>
<Field name="SfUserUserPermissionsChatterAnswersUser">%UserPermissionsChatterAnswersUser</Field>
<Field name="SfUserUserPermissionsInteractionUser">%UserPermissionsInteractionUser</Field>
<Field name="SfUserUserPermissionsKnowledgeUser">%UserPermissionsKnowledgeUser</Field>
<Field name="SfUserUserPermissionsMarketingUser">%UserPermissionsMarketingUser</Field>
<Field name="SfUserUserPermissionsMobileUser">%UserPermissionsMobileUser</Field>
<Field name="SfUserUserPermissionsOfflineUser">%UserPermissionsOfflineUser</Field>
<Field name="SfUserUserPermissionsSFContentUser">%UserPermissionsSFContentUser</Field>
<Field name="SfUserUserPermissionsSiteforceContributorUser">%UserPermissionsSiteforceContributorUser</Field>
<Field name="SfUserUserPermissionsSiteforcePublisherUser">%UserPermissionsSiteforcePublisherUser</Field>
<Field name="SfUserUserPermissionsSupportUser">%UserPermissionsSupportUser</Field>
<Field name="SfUserUserPreferencesActivityRemindersPopup">%UserPreferencesActivityRemindersPopup</Field>
<Field name="SfUserUserPreferencesApexPagesDeveloperMode">%UserPreferencesApexPagesDeveloperMode</Field>
<Field name="SfUserUserPreferencesContentEmailAsAndWhen">%UserPreferencesContentEmailAsAndWhen</Field>
<Field name="SfUserUserPreferencesContentNoEmail">%UserPreferencesContentNoEmail</Field>
<Field name="SfUserUserPreferencesDisCommentAfterLikeEmail">%UserPreferencesDisCommentAfterLikeEmail</Field>
<Field name="SfUserUserPreferencesDisMentionsCommentEmail">%UserPreferencesDisMentionsCommentEmail</Field>
<Field name="SfUserUserPreferencesDisProfPostCommentEmail">%UserPreferencesDisProfPostCommentEmail</Field>
<Field name="SfUserUserPreferencesDisableAllFeedsEmail">%UserPreferencesDisableAllFeedsEmail</Field>
<Field name="SfUserUserPreferencesDisableBookmarkEmail">%UserPreferencesDisableBookmarkEmail</Field>
<Field name="SfUserUserPreferencesDisableChangeCommentEmail">%UserPreferencesDisableChangeCommentEmail</Field>
<Field name="SfUserUserPreferencesDisableFileShareNotificationsForApi">%UserPreferencesDisableFileShareNotificationsForApi</Field>
<Field name="SfUserUserPreferencesDisableFollowersEmail">%UserPreferencesDisableFollowersEmail</Field>
<Field name="SfUserUserPreferencesDisableLaterCommentEmail">%UserPreferencesDisableLaterCommentEmail</Field>
<Field name="SfUserUserPreferencesDisableLikeEmail">%UserPreferencesDisableLikeEmail</Field>
<Field name="SfUserUserPreferencesDisableMentionsPostEmail">%UserPreferencesDisableMentionsPostEmail"</Field>
<Field name="SfUserUserPreferencesDisableMessageEmail">
[UserPreferencesDisableMessageEmail]
</Field>
(Field name="SfUserUserPreferencesDisableProfilePostEmail">
[UserPreferencesDisableProfilePostEmail]
</Field>
(Field name="SfUserUserPreferencesDisableSharePostEmail">
[UserPreferencesDisableSharePostEmail]
</Field>
(Field name="SfUserUserPreferencesEnableAutoSubForFeeds">
[UserPreferencesEnableAutoSubForFeeds]
</Field>
(Field name="SfUserUserPreferencesEventRemindersCheckboxDefault">
[UserPreferencesEventRemindersCheckboxDefault]
</Field>
(Field name="SfUserUserPreferencesHideCSNDesktopTask">
[UserPreferencesHideCSNDesktopTask]
</Field>
(Field name="SfUserUserPreferencesHideCSNGetChatterMobileTask">
[UserPreferencesHideCSNGetChatterMobileTask]
</Field>
(Field name="SfUserUserPreferencesOptOutOfTouch">
[UserPreferencesOptOutOfTouch]
</Field>
(Field name="SfUserUserPreferencesReminderSoundOff">
[UserPreferencesReminderSoundOff]
</Field>
(Field name="SfUserUserPreferencesTaskRemindersCheckboxDefault">
[UserPreferencesTaskRemindersCheckboxDefault]
</Field>
(Field name="SfUserUsername">
[Username]
</Field>
(Field name="SfAttachmentBodyLength">
[BodyLength]
</Field>
(Field name="SfAttachmentDescription">
[Description]
</Field>
(Field name="SfAttachmentId">
[Id]
</Field>
(Field name="SfAttachmentName">
[Name]
</Field>
(Field name="SfCampaignId">
[Parent_Campaign.Id]
</Field>
(Field name="SfCampaignName">
[Parent_Campaign.Name]
</Field>
(Field name="SfCaseId">
[Parent_Case.Id]
</Field>
(Field name="SfCaseName">
[Parent_Case.Name]
</Field>
(Field name="SfContactId">
[Parent_Contact.Id]
</Field>
(Field name="SfContactName">
[Parent_Contact.Name]
</Field>
(Field name="SfContentType">
[ContentType]
</Field>
(Field name="SfContractId">
[Parent_Contract.Id]
</Field>
(Field name="SfContractName">
[Parent_Contract.Name]
</Field>
(Field name="SfEmailTemplateId">
[Parent_EmailTemplate.Id]
</Field>
(Field name="SfEmailTemplateName">
[Parent_EmailTemplate.Name]
</Field>
(Field name="SfEventId">
[Parent_Event.Id]
</Field>
(Field name="SfEventName">
[Parent_Event.Name]
</Field>
(Field name="SfLastModifiedById">
[LastModifiedBy.Id]
</Field>
(Field name="SfLastModifiedByName">
[LastModifiedBy.Name]
</Field>
(Field name="SfLastModifiedDate">
[LastModifiedDate]
</Field>
(Field name="SfLastModifiedDateFiscalQuarter">
[LastModifiedDate_fiscalquarter]
</Field>
(Field name="SfLastModifiedDateFiscalYear">
[LastModifiedDate_fiscalyear]
</Field>
(Field name="SfLeadName">
[Parent_Lead.Name]
</Field>
(Field name="SfLeadId">
[Parent_Lead.Id]
</Field>
(Field name="SfMagic_Item_cId">
[Parent_Magic_Item_c.Id]
</Field>
(Field name="SfMagic_Item_cName">
[Parent_Magic_Item_c.Name]
</Field>
(Field name="SfOpportunityId">
[Parent_Opportunity.Id]
</Field>
(Field name="SfOpportunityName">
[Parent_Opportunity.Name]
</Field>
(Field name="SfOwnerId">
[Owner.Id]
</Field>
(Field name="SfOwnerName">
[Owner.Name]
</Field>
(Field name="SfParentId">
[Parent.Id]
</Field>
(Field name="SfParentName">
[Parent.Name]
</Field>
(Field name="SfProduct2Id">
[Parent_Product2.Id]
</Field>
(Field name="SfProduct2Name">
[Parent_Product2.Name]
</Field>
<?xml version="1.0" encoding="UTF-8" ?>
<Salesforce>
  <CommonMapping>
    <Fields>
      <ContentType>binarydata</ContentType>
      <ModifiedDate>%[LastModifiedDate]</ModifiedDate>
      <CustomFields>
        <CustomField name="sourcetype">Salesforce</CustomField>
        <CustomField name="SfOrganizationId">%[coveo_organization_id]</CustomField>
        <CustomField name="sysauthor">%[Owner.Name]</CustomField>
        <CustomField name="sysdate">%[SystemModstamp]</CustomField>
        <CustomField name="SfSfId">%[Id]</CustomField>
        <CustomField name="SfName">%[Name]</CustomField>
        <CustomField name="SfCreatedDate">%[CreatedDate]</CustomField>
        <CustomField name="SfAccountId">%[Id]</CustomField>
        <CustomField name="SfAccountAnnualRevenue">%[AnnualRevenue]</CustomField>
        <CustomField name="SfAccountAnnualRevenueConverted">%[AnnualRevenue_Converted]</CustomField>
        <CustomField name="SfAccountDescription">%[Description]</CustomField>
        <CustomField name="SfAccountNumber">%[AccountNumber]</CustomField>
        <CustomField name="SfAccountNumberOfEmployees">%[NumberOfEmployees]</CustomField>
        <CustomField name="SfAccountOwnership">%[Ownership]</CustomField>
        <CustomField name="SfAccountPhone">%[Phone]</CustomField>
        <CustomField name="SfAccountRating">%[Rating]</CustomField>
        <CustomField name="SfAccountSic">%[Sic]</CustomField>
        <CustomField name="SfAccountSicDesc">%[SicDesc]</CustomField>
        <CustomField name="SfAccountSite">%[Site]</CustomField>
        <CustomField name="SfAccountSource">%[AccountSource]</CustomField>
        <CustomField name="SfAccountTickerSymbol">%[TickerSymbol]</CustomField>
        <CustomField name="SfAccountType">%[Type]</CustomField>
        <CustomField name="SfAccountWebsite">%[Website]</CustomField>
        <CustomField name="SfCity">%[BillingCity]</CustomField>
        <CustomField name="SfFax">%[Fax]</CustomField>
        <CustomField name="SfIndustry">%[Industry]</CustomField>
        <CustomField name="SfJigsaw">%[Jigsaw]</CustomField>
      </CustomFields>
    </Fields>
  </CommonMapping>
  <Mapping type="Account">
    <Fields>
      <Title>%[Name]</Title>
      <Body>%[Description]</Body>
      <CustomFields>
        <CustomField name="objecttype">Account</CustomField>
        <CustomField name="objecttypename">Account</CustomField>
        <CustomField name="sfinterfaceid">service</CustomField>
        <CustomField name="SfAccountAnnualRevenue">%[AnnualRevenue]</CustomField>
        <CustomField name="SfAccountAnnualRevenueConverted">%[AnnualRevenue_Converted]</CustomField>
        <CustomField name="SfAccountDescription">%[Description]</CustomField>
        <CustomField name="SfAccountId">%[Id]</CustomField>
        <CustomField name="SfAccountNumber">%[AccountNumber]</CustomField>
        <CustomField name="SfAccountNumberOfEmployees">%[NumberOfEmployees]</CustomField>
        <CustomField name="SfAccountOwnership">%[Ownership]</CustomField>
        <CustomField name="SfAccountPhone">%[Phone]</CustomField>
        <CustomField name="SfAccountRating">%[Rating]</CustomField>
        <CustomField name="SfAccountSic">%[Sic]</CustomField>
        <CustomField name="SfAccountSicDesc">%[SicDesc]</CustomField>
        <CustomField name="SfAccountSite">%[Site]</CustomField>
        <CustomField name="SfAccountSource">%[AccountSource]</CustomField>
        <CustomField name="SfAccountTickerSymbol">%[TickerSymbol]</CustomField>
        <CustomField name="SfAccountType">%[Type]</CustomField>
        <CustomField name="SfAccountWebsite">%[Website]</CustomField>
        <CustomField name="SfCity">%[BillingCity]</CustomField>
        <CustomField name="SfFax">%[Fax]</CustomField>
        <CustomField name="SfIndustry">%[Industry]</CustomField>
        <CustomField name="SfJigsaw">%[Jigsaw]</CustomField>
      </CustomFields>
    </Fields>
  </Mapping>
</Salesforce>
<CustomField name="SfParentId">%(Parent.Id)</CustomField>
<CustomField name="SfParentSubject">%(Parent.Subject)</CustomField>
<CustomField name="SfSystemModstamp">%(SystemModstamp)</CustomField>
<CustomField name="SfSystemModstampfq">%(SystemModstamp_fiscalquarter)</CustomField>
<CustomField name="SfSystemModstampfy">%(SystemModstamp_fiscalyear)</CustomField>
<CustomField name="SUUser.Id">%(Owner_User.Id)</CustomField>
<CustomField name="SUUserName">%(Owner_User.Name)</CustomField>
<CustomField name="sysfiletype">SalesforceItem</CustomField>
</CustomFields>
</Fields>
</Mapping>
<Mapping type="CaseComment">
<Fields>
>Title>%(Parent.Subject)</Title>
<Body>%(CommentBody)</Body>
<CustomFields>
<CustomField name="objecttype">Case Comment</CustomField>
<CustomField name="objecttypename">Case Comment</CustomField>
<CustomField name="sfinterfaceid">service</CustomField>
<CustomField name="SfCaseCommentId">%(Id)</CustomField>
<CustomField name="SfCaseId">%(Parent.Id)</CustomField>
<CustomField name="SfCaseNumber">%(Parent.CaseNumber)</CustomField>
<CustomField name="SfCaseSubject">%(Parent.Subject)</CustomField>
<CustomField name="SfCommentBody">%(CommentBody)</CustomField>
<CustomField name="SfIsPublished">%(IsPublished)</CustomField>
<CustomField name="SfLastModifiedById">%(LastModifiedBy.Id)</CustomField>
<CustomField name="SfLastModifiedByName">%(LastModifiedBy.Name)</CustomField>
<CustomField name="SfLastModifiedDate">%(LastModifiedDate)</CustomField>
<CustomField name="SfLastModifiedDatefq">%(LastModifiedDate_fiscalquarter)</CustomField>
<CustomField name="SfLastModifiedDatefy">%(LastModifiedDate_fiscalyear)</CustomField>
<CustomField name="SfSystemModstamp">%(SystemModstamp)</CustomField>
<CustomField name="SfSystemModstampfq">%(SystemModstamp_fiscalquarter)</CustomField>
<CustomField name="SfSystemModstampfy">%(SystemModstamp_fiscalyear)</CustomField>
<CustomField name="sysfiletype">SalesforceItem</CustomField>
</CustomFields>
</Fields>
</Mapping>
<Mapping type="Contact">
<Fields>
>Title>%(Name)</Title>
<Body>%(Description)</Body>
<CustomFields>
<CustomField name="objecttype">Contact</CustomField>
<CustomField name="objecttypename">Contact</CustomField>
<CustomField name="sfinterfaceid">service</CustomField>
<CustomField name="SfAccountId">%(Account.Id)</CustomField>
<CustomField name="SfAccountName">%(Account.Name)</CustomField>
<CustomField name="SfBirthdate">%(Birthdate)</CustomField>
<CustomField name="SfBirthdatefq">%(Birthdate_fiscalquarter)</CustomField>
<CustomField name="SfBirthdatefy">%(Birthdate_fiscalyear)</CustomField>
<CustomField name="SfCity">%(MailingCity)</CustomField>
<CustomField name="SfContactAssistantName">%(AssistantName)</CustomField>
<CustomField name="SfContactAssistantPhone">%(AssistantPhone)</CustomField>
<CustomField name="SfContactDepartment">%(Department)</CustomField>
<CustomField name="SfContactDescription">%(Description)</CustomField>
<CustomField name="SfContactFirstName">%(FirstName)</CustomField>
<CustomField name="SfContactId">%(Id)</CustomField>
<CustomField name="SfContactLastName">%(LastName)</CustomField>
<CustomField name="SfContactName">%(Name)</CustomField>
<CustomField name="SfContactPhone">%(Phone)</CustomField>
<CustomField name="SfContactSalutation">%(Salutation)</CustomField>
<CustomField name="SfContactTitle">%(Title)</CustomField>
<CustomField name="SfCountry">%(MailingCountry)</CustomField>
<CustomField name="SfEmail">%(Email)</CustomField>
<CustomField name="SfEmailDomainName">%(Email_DomainName)</CustomField>
<CustomField name="SfEmailFullDomainName">%(Email_FullDomainName)</CustomField>
<CustomField name="SfFax">%(Fax)</CustomField>
<CustomField name="SfHomePhone">%(HomePhone)</CustomField>
<CustomField name="SfJigsaw">%(Jigsaw)</CustomField>
</CustomFields>
</Fields>
</Mapping>
<CustomField name="SfJigsawContactId">%[JigsawContactId]</CustomField>
<CustomField name="SfLastActivityDate">%[LastActivityDate]</CustomField>
<CustomField name="SfLastActivityDatefq">%[LastActivityDate_fiscalquarter]</CustomField>
<CustomField name="SfLastActivityDatefyear">%[LastActivityDate_fiscalyear]</CustomField>
<CustomField name="SfLastModifiedById">%[LastModifiedBy.Id]</CustomField>
<CustomField name="SfLastModifiedByName">%[LastModifiedBy.Name]</CustomField>
<CustomField name="SfLastModifiedDate">%[LastModifiedDate]</CustomField>
<CustomField name="SfLastModifiedDatefq">%[LastModifiedDate_fiscalquarter]</CustomField>
<CustomField name="SfLastModifiedDatefyear">%[LastModifiedDate_fiscalyear]</CustomField>
<CustomField name="SfLeadSource">%[LeadSource]</CustomField>
<CustomField name="SfMasterRecordId">%[MasterRecord.Id]</CustomField>
<CustomField name="SfMasterRecordName">%[MasterRecord.Name]</CustomField>
<CustomField name="SfMobilePhone">%[MobilePhone]</CustomField>
<CustomField name="SfOwnerId">%[Owner.Id]</CustomField>
<CustomField name="SfOwnerName">%[Owner.Name]</CustomField>
<CustomField name="SfPostalCode">%[MailingPostalCode]</CustomField>
<CustomField name="SfReportsToId">%[ReportsTo.Id]</CustomField>
<CustomField name="SfReportsToName">%[ReportsTo.Name]</CustomField>
<CustomField name="SfState">%[MailingState]</CustomField>
<CustomField name="SfStreet">%[MailingStreet]</CustomField>
<CustomField name="SfSystemModstamp">%[SystemModstamp]</CustomField>
<CustomField name="SfSystemModstampfq">%[SystemModstamp_fiscalquarter]</CustomField>
<CustomField name="SfSystemModstampfyear">%[SystemModstamp_fiscalyear]</CustomField>
<CustomField name="sysfiletype">SalesforceItem</CustomField>
</CustomFields>
</Fields>
</Mapping>

<Fields>
  <Title><![CDATA[Subject]]></Title>
  <Body><![CDATA[ActivityDate]]></Body>
</Fields>
</Mapping type="Event">
<Fields>
  <objecttype>Event</objecttype>
  <objecttypename>Event</objecttypename>
  <service></service>
  <Account.Id>%[Account.Id]</Account.Id>
  <Account.Name>%[Account.Name]</Account.Name>
  <ActivityDate>%[ActivityDate]</ActivityDate>
  <ActivityDatefq>%[ActivityDate_fiscalquarter]</ActivityDatefq>
  <ActivityDatefyear>%[ActivityDate_fiscalyear]</ActivityDatefyear>
  <Asset.Id>%[Asset.Id]</Asset.Id>
  <Asset.Name>%[Asset.Name]</Asset.Name>
  <Contact.Id>%[Contact.Id]</Contact.Id>
  <Contact.Name>%[Contact.Name]</Contact.Name>
  <Contract.Id>%[Contract.Id]</Contract.Id>
  <EndDateDateTime>%[EndDateDateTime]</EndDateDateTime>
  <EndDateDateTimefyear>%[EndDateDateTime_fiscalyear]</EndDateDateTimefyear>
  <GroupId>%[GroupId]</GroupId>
  <GroupId>%[GroupId]</GroupId>
  <GroupName>%[GroupName]</GroupName>
  <GroupEventType>%[GroupEventType]</GroupEventType>
  <IsAllDayEvent>%[IsAllDayEvent]</IsAllDayEvent>
  <IsChild>%[IsChild]</IsChild>
  <IsReminderDate>%[IsReminderDate]</IsReminderDate>
  <IsReminderDatefq>%[IsReminderDate_fiscalquarter]</IsReminderDatefq>
  <IsReminderDatefyear>%[IsReminderDate_fiscalyear]</IsReminderDatefyear>
  <StartDateDateTime>%[StartDateDateTime]</StartDateDateTime>
  <StartDateDateTimefq>%[StartDateDateTime_fiscalquarter]</StartDateDateTimefq>
</Fields>
<CustomField name="SfUserDivision">%(Division)</CustomField>
<CustomField name="SfUserEmailEncodingKey">%(EmailEncodingKey)</CustomField>
<CustomField name="SfUserEmployeeNumber">%(EmployeeNumber)</CustomField>
<CustomField name="SfUserExtension">%(Extension)</CustomField>
<CustomField name="SfUserFederationIdentifier">%(FederationIdentifier)</CustomField>
<CustomField name="SfUserFirstName">%(FirstName)</CustomField>
<CustomField name="SfUserForecastEnabled">%(ForecastEnabled)</CustomField>
<CustomField name="SfUserId">%(Id)</CustomField>
<CustomField name="SfUserLastName">%(LastName)</CustomField>
<CustomField name="SfUserLocaleSidKey">%(LocaleSidKey)</CustomField>
<CustomField name="SfUserName">%(Name)</CustomField>
<CustomField name="SfUserPhone">%(Phone)</CustomField>
<CustomField name="SfUserReceivesAdminInfoEmails">%(ReceivesAdminInfoEmails)</CustomField>
<CustomField name="SfUserReceivesInfoEmails">%(ReceivesInfoEmails)</CustomField>
<CustomField name="SfUserRole.Id">%(UserRole.Id)</CustomField>
<CustomField name="SfUserRole.Name">%(UserRole.Name)</CustomField>
<CustomField name="SfUserTimezoneSidKey">%(TimeZoneSidKey)</CustomField>
<CustomField name="SfUserTitle">%(Title)</CustomField>
<CustomField name="SfUserUserPermissionsCallCenterAutoLogin">%(UserPermissionsCallCenterAutoLogin)</CustomField>
<CustomField name="SfUserUserPermissionsChatterAnswersSUser">%(UserPermissionsChatterAnswersSUser)</CustomField>
<CustomField name="SfUserUserPermissionsInteractionUser">%(UserPermissionsInteractionUser)</CustomField>
<CustomField name="SfUserUserPermissionsKnowledgeUser">%(UserPermissionsKnowledgeUser)</CustomField>
<CustomField name="SfUserUserPermissionsMobileUser">%(UserPermissionsMobileUser)</CustomField>
<CustomField name="SfUserUserPermissionsOfflineUser">%(UserPermissionsOfflineUser)</CustomField>
<CustomField name="SfUserUserPermissionsSFContentUser">%(UserPermissionsSFContentUser)</CustomField>
<CustomField name="SfUserUserPermissionsSiteforceContributorUser">%(UserPermissionsSiteforceContributorUser)</CustomField>
<CustomField name="SfUserUserPermissionsSiteforcePublisherUser">%(UserPermissionsSiteforcePublisherUser)</CustomField>
<CustomField name="SfUserUserPermissionsSupportUser">%(UserPermissionsSupportUser)</CustomField>
<CustomField name="SfUserUserPreferencesActivityRemindersPopup">%(UserPreferencesActivityRemindersPopup)</CustomField>
<CustomField name="SfUserUserPreferencesApexPagesDeveloperMode">%(UserPreferencesApexPagesDeveloperMode)</CustomField>
<CustomField name="SfUserUserPreferencesContentEmailAsAndWhen">%(UserPreferencesContentEmailAsAndWhen)</CustomField>
<CustomField name="SfUserUserPreferencesContentNoEmail">%(UserPreferencesContentNoEmail)</CustomField>
<CustomField name="SfUserUserPreferencesDisCommentAfterLikeEmail">%(UserPreferencesDisCommentAfterLikeEmail)</CustomField>
<CustomField name="SfUserUserPreferencesDisMentionsCommentEmail">%(UserPreferencesDisMentionsCommentEmail)</CustomField>
<CustomField name="SfUserUserPreferencesDisProfPostCommentEmail">%(UserPreferencesDisProfPostCommentEmail)</CustomField>
<CustomField name="SfUserUserPreferencesDisableAllFeedsEmail">%(UserPreferencesDisableAllFeedsEmail)</CustomField>
<CustomField name="SfUserUserPreferencesDisableBookmarkEmail">%(UserPreferencesDisableBookmarkEmail)</CustomField>
<CustomField name="SfUserUserPreferencesDisableChangeCommentEmail">%(UserPreferencesDisableChangeCommentEmail)</CustomField>
<CustomField name="SfUserUserPreferencesDisableFileShareNotificationsForApi">%(UserPreferencesDisableFileShareNotificationsForApi)</CustomField>
<CustomField name="SfUserUserPreferencesDisableFollowersEmail">%(UserPreferencesDisableFollowersEmail)</CustomField>
<CustomField name="SfUserUserPreferencesDisableLaterCommentEmail">%(UserPreferencesDisableLaterCommentEmail)</CustomField>
<CustomField name="SfUserUserPreferencesDisableLikeEmail">%(UserPreferencesDisableLikeEmail)</CustomField>
<CustomField name="SfUserUserPreferencesDisableMentionsPostEmail">%(UserPreferencesDisableMentionsPostEmail)</CustomField>
<CustomField name="SfUserUserPreferencesDisableFollowersEmail">%(UserPreferencesDisableFollowersEmail)</CustomField>
<CustomField name="SfUserUserPreferencesDisableLaterCommentEmail">%(UserPreferencesDisableLaterCommentEmail)</CustomField>
<CustomField name="SfUserUserPreferencesDisableLikeEmail">%(UserPreferencesDisableLikeEmail)</CustomField>
9.38.9.2 Salesforce Mapping File Example for Knowledge Base

When your Salesforce organization includes Knowledge Base articles and you want to index their content, you must include additional mappings for Knowledge content types.

The mapping file example presented in this topic maps two arbitrary named Knowledge Base objects:

- **MyKBArticleType1**
- **MyKBArticleType2**

```xml
<?xml version="1.0" encoding="UTF-8"?>
<Mappings>
  <Version>1</Version>
  <CommonMapping>
    <Field name="sourceType">Salesforce</Field> 
    <Field name="sfOrganizationId">%\[coveo_organization_id\]<\Field>
    <Field name="sysauthor">%\[kav_CreatedBy.Name\]<\Field>
    <Field name="sysdate">%\[kav_LastPublishedDate\]<\Field>
    <Field name="sysSfId">%\[ka_id\]<\Field>
    <Field name="sfId">%\[ka_id\]<\Field>
    <Field name="sfRId">%\[ka_id\]<\Field>
    <Field name="sfdcCreatedDate">%\[kav_CreatedDate\]<\Field>
    <Field name="sfdcCreatedById">%\[kav_CreatedById\]<\Field>
    <Field name="sfdcIsDeleted">%\[kav_IsDeleted\]<\Field>
  </CommonMapping>
</Mappings>
```
<Field name="SFParticipantId">%{ka_CreatedById};%{kv_LastModifiedById};</Field>
<Field name="SfParticipantName">%{CreatedByName};%{kv_LastModifiedById};</Field>
</Fields>
</CommonMapping>
</Mapping type="MyKBArticleType1">
<Title>%{kav_Title}</Title>
</Body>%{kv_Summary}</Body>
</Fields>
</Mapping type="MyKBArticleType2">
<Title>%{kav_Title}</Title>
</Body>%{kv_Summary}</Body>
</Fields>
</Mapping type="MyKBArticleType2">
<Title>%{kav_Title}</Title>
</Body>%{kv_Summary}</Body>
</Fields>
<table>
<thead>
<tr>
<th>Field Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SfKbLastPublishedDate</td>
<td>Last Published Date</td>
</tr>
<tr>
<td>SfKbLastPublishedDatefq</td>
<td>Fiscal Quarterly Published Date</td>
</tr>
<tr>
<td>SfKbLastPublishedDatefy</td>
<td>Fiscal Year Published Date</td>
</tr>
<tr>
<td>SfKbPublishStatus</td>
<td>Publish Status</td>
</tr>
<tr>
<td>SfKbRecipeC</td>
<td>Recipe C</td>
</tr>
<tr>
<td>SfKbSummary</td>
<td>Summary</td>
</tr>
<tr>
<td>SfKbTitle</td>
<td>Title</td>
</tr>
<tr>
<td>SfKbUrlName</td>
<td>URL Name</td>
</tr>
<tr>
<td>SfKbVersionNumber</td>
<td>Version Number</td>
</tr>
<tr>
<td>SfLanguage</td>
<td>Language</td>
</tr>
<tr>
<td>SfLastModifiedById</td>
<td>Last Modified By Id</td>
</tr>
<tr>
<td>SfLastModifiedByName</td>
<td>Last Modified By Name</td>
</tr>
<tr>
<td>SfLastModifiedDate</td>
<td>Last Modified Date</td>
</tr>
<tr>
<td>SfLastModifiedDatefq</td>
<td>Fiscal Quarterly Modified Date</td>
</tr>
<tr>
<td>SfLastModifiedDatefy</td>
<td>Fiscal Year Modified Date</td>
</tr>
<tr>
<td>SfSystemModstamp</td>
<td>System Modstamp</td>
</tr>
<tr>
<td>SfSystemModstampfq</td>
<td>Fiscal Quarterly System Modstamp</td>
</tr>
<tr>
<td>SfSystemModstampfy</td>
<td>Fiscal Year System Modstamp</td>
</tr>
<tr>
<td>sysfiletype</td>
<td>Salesforce Item</td>
</tr>
</tbody>
</table>

CES 7.0.7022 – (September 2014)

<?xml version="1.0" encoding="UTF-8" ?>
<Salesforce>
  <CommonMapping>
    <Fields>
      <ContentType>binarydata</ContentType>
      <ModifiedDate>%[LastModifiedDate]</ModifiedDate>
      <CustomFields>
        <CustomField name="sourcetype">Salesforce</CustomField>
        <CustomField name="SfChannelsFlagMerged">Internal App:%[kav_IsVisibleInApp];Customer Portal:%[kav_IsVisibleInCsp];Public Knowledge Base:%[kav_IsVisibleInPkb];Partner Portal:%[kav_IsVisibleInPrm];</CustomField>
        <CustomField name="SfOrganizationId">%[coveo_organization_id]</CustomField>
        <CustomField name="sysauthor">%[kav_CreatedBy.Name]</CustomField>
        <CustomField name="sysSfId">%[ka_id]</CustomField>
        <CustomField name="SfId">%[ka_id]</CustomField>
        <CustomField name="SfKbId">%[ka_id]</CustomField>
        <CustomField name="SfCreatedByName">%[kav_CreatedBy.Name]</CustomField>
        <CustomField name="SfKbArchivedDate">%[ka_ArchivedDate]</CustomField>
        <CustomField name="SfKbArchivedDatefq">%[ka_ArchivedDate_fiscalquarter]</CustomField>
        <CustomField name="SfKbArchivedDatefy">%[ka_ArchivedDate_fiscalyear]</CustomField>
        <CustomField name="SfKbArticleNumber">%[kav_ArticleNumber]</CustomField>
        <CustomField name="SfKbCaseAssociationCount">%[ka_CaseAssociationCount]</CustomField>
    </CustomFields>
  </Fields>
</CommonMapping>

<Mapping type="MyKBArticleType1">
  <Fields>
    <Title>%[kav_Title]</Title>
    <Body>%[kav_Summary]</Body>
    <CustomFields>
      <CustomField name="objecttype">MyKBArticleType1</CustomField>
      <CustomField name="objecttypename">My KB Article Type1</CustomField>
      <CustomField name="sfinterfaceid">kb</CustomField>
      <CustomField name="SfCaseId">%[ka_CaseArticles.CaseId]</CustomField>
      <CustomField name="SfCreatedByByName">%[kav_CreatedBy.Name]</CustomField>
      <CustomField name="SfKbArchivedDatefq">%[ka_ArchivedDate_fiscalquarter]</CustomField>
      <CustomField name="SfKbArchivedDatefy">%[ka_ArchivedDate_fiscalyear]</CustomField>
      <CustomField name="SfKbArticleNumber">%[kav_ArticleNumber]</CustomField>
      <CustomField name="SfKbCaseAssociationCount">%[ka_CaseAssociationCount]</CustomField>
    </CustomFields>
  </Fields>
</Mapping>
9.38.9.3 Salesforce Mapping File Example for CRM Content

With Salesforce CRM Content you can organize, share, search, and manage content within your organization and across key areas of the Salesforce application. Content can include all file types, from traditional business documents such as Microsoft PowerPoint presentations to audio files, video files, Web pages, and Google docs (see the Salesforce document Salesforce CRM Content Overview).

When your Salesforce organization includes CRM content and you want to index the content of these files, you must include additional mappings for CRM content type.

The following Salesforce CRM content mapping file example is a good starting point.

```xml
<?xml version="1.0" encoding="UTF-8"?>
<Mappings>
  <Version>1</Version>
  <CommonMapping>
    <Fields>
      <Field name="sourcetype">Salesforce</Field>
      <Field name="SfOrganizationId">%{coveo_organization_id}</Field>
      <Field name="sysauthor">%{Owner.Name}</Field>
      <Field name="sysdate">%{SystemModstamp}</Field>
      <Field name="sysSfId">%{Id}</Field>
      <Field name="SfId">%{Id}</Field>
      <Field name="SfName">%{Name}</Field>
      <Field name="SfCreatedDate">%{CreatedDate}</Field>
      <Field name="SfCreatedByName">%{CreatedBy.Name}</Field>
      <Field name="SfCreatedById">%{CreatedBy.Id}</Field>
      <Field name="SfIsDeleted">%{IsDeleted}</Field>
      <Field name="SfParticipantId">%{CreatedBy.Id};%{Owner.Id};%{LastModifiedBy.Id};%{Contact.Id}</Field>
      <Field name="SfParticipantName">%{CreatedBy.Name};%{Owner.Name};%{LastModifiedBy.Name};%{Contact.Name}</Field>
    </Fields>
  </CommonMapping>
</Mappings>
```

(CES 7.0.7104+ (October 2014))
<Field name="SFCollaborationGroupId">%FirstPublishLocation_CollaborationGroupId</Field>
<Field name="SFCollaborationGroupName">%FirstPublishLocation_CollaborationGroupName</Field>
<Field name="SFCollaborationGroupId">%FirstPublishLocation_CollaborationGroupId</Field>
<Field name="SFCollaborationGroupName">%FirstPublishLocation_CollaborationGroupName</Field>
<Field name="SFContactId">%FirstPublishLocation_Contact_Id</Field>
<Field name="SFContactName">%FirstPublishLocation_Contact_Name</Field>
<Field name="SFContentDocumentId">%ContentDocument_Id</Field>
<Field name="SFContentDocumentTitle">%ContentDocument_Title</Field>
<Field name="SFContentModifiedDate">%ContentModifiedDate</Field>
<Field name="SFContentModifiedDate">%ContentModifiedDate</Field>
<Field name="SFContentModifiedDate_fiscalquarter">%ContentModifiedDate_fiscalquarter</Field>
<Field name="SFContentModifiedDate_fiscalyear">%ContentModifiedDate_fiscalyear</Field>
<Field name="SFContentSize">%ContentSize</Field>
<Field name="SFContentUrl">%ContentUrl</Field>
<Field name="SFContentVersionId">%Id</Field>
<Field name="SFContentVersionIsLatest">%IsLatest</Field>
<Field name="SFContentVersionOrigin">%Origin</Field>
<Field name="SFContentVersionPublishStatus">%PublishStatus</Field>
<Field name="SFContentVersionTitle">%Title</Field>
<Field name="SFContractId">%FirstPublishLocation_Contract_Id</Field>
<Field name="SFContractName">%FirstPublishLocation_Contract_Name</Field>
<Field name="SFDashboardComponentId">%FirstPublishLocation_DashboardComponent_Id</Field>
<Field name="SFDashboardComponentName">%FirstPublishLocation_DashboardComponent_Name</Field>
<Field name="SFDashboardId">%FirstPublishLocation_Dashboard_Id</Field>
<Field name="SFDashboardName">%FirstPublishLocation_Dashboard_Name</Field>
<Field name="SFEventId">%FirstPublishLocation_Event_Id</Field>
<Field name="SFEventName">%FirstPublishLocation_Event_Name</Field>
<Field name="SFFirstPublishLocationId">%FirstPublishLocation_Id</Field>
<Field name="SFLastModifiedByDate">%LastModifiedBy_Date</Field>
<Field name="SFLastModifiedByDate_fiscalquarter">%LastModifiedBy_Date_fiscalquarter</Field>
<Field name="SFLastModifiedByDate_fiscalyear">%LastModifiedBy_Date_fiscalyear</Field>
<Field name="SFLastModifiedById">%LastModifiedById</Field>
<Field name="SFLastModifiedByName">%LastModifiedBy_Name</Field>
<Field name="SFLastModifiedDate">%LastModifiedDate</Field>
<Field name="SFLastModifiedDate_fiscalquarter">%LastModifiedDate_fiscalquarter</Field>
<Field name="SFLastModifiedDate_fiscalyear">%LastModifiedDate_fiscalyear</Field>
<Field name="SFLeadId">%FirstPublishLocation_Lead_Id</Field>
<Field name="SFLeadName">%FirstPublishLocation_Lead_Name</Field>
<Field name="SFLastScroll_kaid">%FirstPublishLocation_LastScroll_ka_Id</Field>
<Field name="SFLastScroll_kaName">%FirstPublishLocation_LastScroll_ka_Name</Field>
<Field name="SFMagic_Item_cId">%FirstPublishLocation_Magic_Item_c_Id</Field>
<Field name="SFMagic_Item_cName">%FirstPublishLocation_Magic_Item_c_Name</Field>
<Field name="SFMagic_Spell_kaid">%FirstPublishLocation_Magic_Spell_ka_Id</Field>
<Field name="SFMagic_Spell_kaName">%FirstPublishLocation_Magic_Spell_ka_Name</Field>
<Field name="SFOpportunityId">%FirstPublishLocation_Opportunity_Id</Field>
<Field name="SFOpportunityName">%FirstPublishLocation_Opportunity_Name</Field>
<Field name="SFOwnerId">%Owner_Id</Field>
<Field name="SFOwnerName">%Owner_Name</Field>
<Field name="SFProduct2Id">%FirstPublishLocation_Product2_Id</Field>
<Field name="SFProduct2Name">%FirstPublishLocation_Product2_Name</Field>
<Field name="SFReportId">%FirstPublishLocation_Report_Id</Field>
<Field name="SFReportName">%FirstPublishLocation_Report_Name</Field>
<Field name="SFSiteId">%FirstPublishLocation_Site_Id</Field>
<Field name="SFSiteName">%FirstPublishLocation_Site_Name</Field>
<Field name="SSFolutionId">%FirstPublishLocation_Solution_Id</Field>
<Field name="SSFolutionName">%FirstPublishLocation_Solution_Name</Field>
<Field name="SSFSystemModstamp">%[SystemModstamp]_</Field>
<Field name="SSFSystemModstampf">%[SystemModstamp_fiscalquarter]_</Field>
<Field name="SSFSystemModstampfq">%[SystemModstamp_fiscalyear]_</Field>
<Field name="STaskId">%FirstPublishLocation_Task_Id</Field>
<Field name="STaskName">%FirstPublishLocation_Task_Name</Field>
<Field name="SFUserId">%FirstPublishLocation_User_Id</Field>
<Field name="SFUserName">%FirstPublishLocation_User_Name</Field>
<?xml version="1.0" encoding="UTF-8" ?>
<Salesforce>
  <CommonMapping>
    <Fields>
      <ContentType>binarydata</ContentType>
      <ModifiedDate>%[LastModifiedDate]</ModifiedDate>
      <CustomFields>
        <CustomField name="sourcetype">Salesforce</CustomField>
        <CustomField name="sorganizationId">%coveo_organization_id</CustomField>
        <CustomField name="sysauthor">%[Owner.Name]</CustomField>
        <CustomField name="sysdate">%[SystemModstamp]</CustomField>
        <CustomField name="sfId">%[Id]</CustomField>
        <CustomField name="SfCreatedDate">%[CreatedDate]</CustomField>
        <CustomField name="SfCreatedByName">%[CreatedBy.Name]</CustomField>
        <CustomField name="SfCreatedById">%[CreatedBy.Id]</CustomField>
        <CustomField name="SfIsDeleted">%[IsDeleted]</CustomField>
        <CustomField name="SfParticipantId">%[ParticipantId]</CustomField>
        <CustomField name="SfParticipantName">%[ParticipantName]</CustomField>
        <CustomField name="objecttype">ContentVersion</objecttype>
        <ContentType>Content</ContentType>
        <ModifiedDate>%[ContentModifiedDate]</ModifiedDate>
        <CustomFields>
          <CustomField name="objecttypename">Content</CustomField>
          <CustomField name="sfinterfaceid">standard</CustomField>
          <CustomField name="SfAccountId">%[FirstPublishLocation_Account.Id]</CustomField>
          <CustomField name="SfAccountName">%[FirstPublishLocation_Account.Name]</CustomField>
          <CustomField name="SfAssetId">%[FirstPublishLocation_Asset.Id]</CustomField>
          <CustomField name="SfAssetName">%[FirstPublishLocation_Asset.Name]</CustomField>
          <CustomField name="SfCampaignId">%[FirstPublishLocation_Campaign.Id]</CustomField>
          <CustomField name="SfCampaignName">%[FirstPublishLocation_Campaign.Name]</CustomField>
          <CustomField name="SfCaseId">%[FirstPublishLocation_Case.Id]</CustomField>
          <CustomField name="SfCaseName">%[FirstPublishLocation_Case.Name]</CustomField>
          <CustomField name="SfCollaborationGroupId">%[FirstPublishLocation_CollaborationGroup.Id]</CustomField>
          <CustomField name="SfCollaborationGroupName">%[FirstPublishLocation_CollaborationGroup.Name]</CustomField>
          <CustomField name="SfContactId">%[FirstPublishLocation_Contact.Id]</CustomField>
          <CustomField name="SfContactName">%[FirstPublishLocation_Contact.Name]</CustomField>
          <CustomField name="SfDocumentId">%[ContentDocument.Id]</CustomField>
          <CustomField name="SfDocumentTitle">%[ContentDocument.Title]</CustomField>
          <CustomField name="SfDocumentModifiedDate">%[ContentDocumentModifiedDate]</CustomField>
          <CustomField name="SfDocumentModifiedDatefq">%[ContentDocumentModifiedDate_fiscalquarter]</CustomField>
          <CustomField name="SfDocumentModifiedDatefgy">%[ContentDocumentModifiedDate_fiscalyear]</CustomField>
          <CustomField name="SfContentSize">%[ContentSize]</CustomField>
          <CustomField name="SfContentUrl">%[ContentUrl]</CustomField>
          <CustomField name="SfContentVersionId">%[Id]</CustomField>
          <CustomField name="SfContentVersionIsLatest">%[IsLatest]</CustomField>
          <CustomField name="SfContentVersionOrigin">%[Origin]</CustomField>
          <CustomField name="SfContentVersionPublishStatus">%[PublishStatus]</CustomField>
          <CustomField name="SfContentVersionTitle">%[VersionTitle]</CustomField>
          <CustomField name="SfContentWorkspaceId">%[FirstPublishLocation_ContentWorkspace.Id]</CustomField>
          <CustomField name="SfContentWorkspaceName">%[FirstPublishLocation_ContentWorkspace.Name]</CustomField>
          <CustomField name="SfContractId">%[FirstPublishLocation_Contract.Id]</CustomField>
          <CustomField name="SfContractName">%[FirstPublishLocation_Contract.Name]</CustomField>
          <CustomField name="SfDashboardComponentId">%[FirstPublishLocation_DashboardComponent.Id]</CustomField>
          <CustomField name="SfDashboardComponentName">%[FirstPublishLocation_DashboardComponent.Name]</CustomField>
          <CustomField name="SfDashboardId">%[FirstPublishLocation_Dashboard.Id]</CustomField>
        </CustomFields>
      </Fields>
    </CommonMapping>
  </Mapping type="ContentVersion">
    <Fields>
      <Title>%[Title]</Title>
      <CustomFields>
        <CustomField name="objecttype">ContentVersion</objecttype>
        <ContentType>Content</ContentType>
        <ModifiedDate>%[ContentModifiedDate]</ModifiedDate>
        <CustomFields>
          <CustomField name="objecttypename">Content</CustomField>
          <CustomField name="sfinterfaceid">standard</CustomField>
          <CustomField name="SfAccountId">%[FirstPublishLocation_Account.Id]</CustomField>
          <CustomField name="SfAccountName">%[FirstPublishLocation_Account.Name]</CustomField>
          <CustomField name="SfAssetId">%[FirstPublishLocation_Asset.Id]</CustomField>
          <CustomField name="SfAssetName">%[FirstPublishLocation_Asset.Name]</CustomField>
          <CustomField name="SfCampaignId">%[FirstPublishLocation_Campaign.Id]</CustomField>
          <CustomField name="SfCampaignName">%[FirstPublishLocation_Campaign.Name]</CustomField>
          <CustomField name="SfCaseId">%[FirstPublishLocation_Case.Id]</CustomField>
          <CustomField name="SfCaseName">%[FirstPublishLocation_Case.Name]</CustomField>
          <CustomField name="SfCollaborationGroupId">%[FirstPublishLocation_CollaborationGroup.Id]</CustomField>
          <CustomField name="SfCollaborationGroupName">%[FirstPublishLocation_CollaborationGroup.Name]</CustomField>
          <CustomField name="SfContactId">%[FirstPublishLocation_Contact.Id]</CustomField>
          <CustomField name="SfContactName">%[FirstPublishLocation_Contact.Name]</CustomField>
          <CustomField name="SfDocumentId">%[ContentDocument.Id]</CustomField>
          <CustomField name="SfDocumentTitle">%[ContentDocument.Title]</CustomField>
          <CustomField name="SfDocumentModifiedDate">%[ContentDocumentModifiedDate]</CustomField>
          <CustomField name="SfDocumentModifiedDatefq">%[ContentDocumentModifiedDate_fiscalquarter]</CustomField>
          <CustomField name="SfDocumentModifiedDatefgy">%[ContentDocumentModifiedDate_fiscalyear]</CustomField>
          <CustomField name="SfContentSize">%[ContentSize]</CustomField>
          <CustomField name="SfContentUrl">%[ContentUrl]</CustomField>
          <CustomField name="SfContentVersionId">%[Id]</CustomField>
          <CustomField name="SfContentVersionIsLatest">%[IsLatest]</CustomField>
          <CustomField name="SfContentVersionOrigin">%[Origin]</CustomField>
          <CustomField name="SfContentVersionPublishStatus">%[PublishStatus]</CustomField>
          <CustomField name="SfContentVersionTitle">%[VersionTitle]</CustomField>
          <CustomField name="SfContentWorkspaceId">%[FirstPublishLocation_ContentWorkspace.Id]</CustomField>
          <CustomField name="SfContentWorkspaceName">%[FirstPublishLocation_ContentWorkspace.Name]</CustomField>
          <CustomField name="SfContractId">%[FirstPublishLocation_Contract.Id]</CustomField>
          <CustomField name="SfContractName">%[FirstPublishLocation_Contract.Name]</CustomField>
          <CustomField name="SfDashboardComponentId">%[FirstPublishLocation_DashboardComponent.Id]</CustomField>
          <CustomField name="SfDashboardComponentName">%[FirstPublishLocation_DashboardComponent.Name]</CustomField>
          <CustomField name="SfDashboardId">%[FirstPublishLocation_Dashboard.Id]</CustomField>
        </CustomFields>
      </Fields>
    </Mapping type="ContentVersion">
</Salesforce>
CES 9.38.9.4 Salesforce Mapping File Example for Chatter Objects

Chatter feed items appear in various Salesforce objects. You can make the content of Chatter feed searchable. Once the Chatter objects are available (see "Salesforce ObjectsToGet Configuration File Example for Chatter Objects" on page 1491), you must include appropriate mappings for these Chatter objects and fields.

The following Chatter mapping file example is a good starting point.

CES 7.0.7104+ (October 2014)

```xml
<Version>1</Version>
<Mappings>
  <Mapping type="FeedItem">
    <Title><![CDATA[%(Title)]]></Title>
    <Body><![CDATA[%(Body)]]></Body>
    <Fields>
      <Field name="sysfiletype">FeedItem</Field>
    </Fields>
  </Mapping>
</Mappings>
```
CES 7.0.7022–(September 2014)

<?xml version="1.0" encoding="utf-8"?>
<Salesforce>
  <Mapping type="FeedItem">
    <Fields>
      <Title>%[Title]</Title>
      <Body>%[LinkUrl] %[Body]</Body>
      <CustomFields>
        <CustomField name="sysfiletype">FeedItem</CustomField>
      </CustomFields>
    </Fields>
  </Mapping>
  <Mapping type="FeedComment">
    <Fields>
      <Title>Comment by %[CreatedBy.Name]</Title>
      <Body>%[CommentBody]</Body>
      <CustomFields>
        <CustomField name="sysfiletype">FeedComment</CustomField>
      </CustomFields>
    </Fields>
  </Mapping>
  <Mapping type="ContentVersion">
    <Fields>
      <Title>%[Title]</Title>
      <CustomFields>
        <CustomField name="sysfiletype">ContentVersion</CustomField>
      </CustomFields>
    </Fields>
  </Mapping>
</Salesforce>
FeedComment can have access to information on the FeedItem:

1. In your ObjectToGet configuration file, add all needed FeedItem fields [i.e. NetworkScope (\texttt{<string>NetworkScope</string>})] on a FeedComment (see FeedItem Fields).
2. In your Salesforce mapping file, add all needed mappings on the FeedComment with a FeedItem.[Field] relationship [i.e. \texttt{<Field name="SFFeedItemNetworkScope">%\{FeedItem.NetworkScope\]}</Field>]} (see FeedItem Fields).
3. Add the custom field(s) in your Salesforce field set [i.e. \texttt{SFFeedItemNetworkScope}].
4. On the Coveo server, access the Administration Tool.
5. Rebuild the Salesforce source.

In a search interface, all needed FeedItem information appear on a FeedComment record.

9.38.10 Configuring a Salesforce Security Provider

A Salesforce source requires a Salesforce security provider to index permissions on Salesforce items so that when end-users search for Salesforce content, in search results, they only see Salesforce items that they have permissions to see.

Notes:

- You do not need to perform this procedure when you want to index Knowledge Base articles. It is not possible to index Knowledge Base permissions so no Salesforce security providers is needed.
- You can get familiar with how Coveo components deal with permissions on documents both at indexing and query time.

To configure a Salesforce security provider

1. On the Coveo server, access the Administration Tool.
3. In the navigation panel on the left, select Security Providers.
5. In the Modify Security Provider page:
a. In the **Name** box, enter a name of your choice for your Salesforce security provider.

b. In the **Security Provider Type** list, select Salesforce.

   **Note: CES 7.0.5639– (July 2013)** The Salesforce item corresponds to the source type now identified as Salesforce (Legacy).

c. In the **User Identity** list, select the user identity that you created for the Salesforce organization that you want to index (see "Creating a Salesforce User Identity" on page 1449).

d. In the **Client Id** box, paste the Customer Key value that you obtained earlier (see "Getting Salesforce Client_ID and Client_Secret Values" on page 1453).

e. In the **Client Secret** box, paste the Customer Secret value that you obtained earlier (see "Getting Salesforce Client_ID and Client_Secret Values" on page 1453).

f. Select the **Sandbox** check box only when you want to use this security provider with a source for a
Salesforce sandbox (test.salesforce.com) rather than for your Salesforce production environment (login.salesforce.com).

- Leave the **Use Refresh Token** check box cleared unless you want to use the refresh token authentication method. This method is typically used when an application configures the security provider (such as in the Coveo cloud platform).

- In the **Working Folder** box, you can change the default security provider working folder path (C:\tmp) when for example your Coveo server is equipped with a separate hard disk for temporary files.

- In the **Security Cache Refresh Frequency** box, consider changing the time interval (in minutes) at which the internal cache of the Salesforce security provider is refreshed. The default value is 60 minutes.

  The Salesforce security provider must refresh its internal cache to maintain the freshness of the Salesforce data used when the security cache is updated (see "Refreshing Security Caches" on page 266).

  **Example:** The internal cache of the Salesforce security provider contains the user profiles. If the profile of a user changes in Salesforce, the internal cache of the security provider must first be refreshed to make this change available for the next security cache update.

  Consider increasing the **Security Cache Refresh Frequency** value when you have more than 100,000 users. The rule of thumb is 60 minutes per 100,000 users.

  It is not recommended to reduce the value below 60 minutes to prevent increasing too much the number of API calls made to Salesforce.

- In the **Email Security Provider** list, select the Email, Active Directory, or custom security provider that you created earlier (see Salesforce Connector Deployment Overview).

- Leave the **Allow Complex Identities** option cleared as it does not apply to this type of security provider.

- Click **Apply Changes**.

**What's Next?**

Create your Salesforce source (see "Configuring and Indexing a Salesforce Source" on page 1536).

**9.38.11 Configuring and Indexing a Salesforce Source**

A source defines a set of configuration parameters for a specific Salesforce database.

**Note:** When you have access to more than one Salesforce organization, you must define one source for each Salesforce organization that you want to index.

To configure and index a Salesforce source

1. On the Coveo server, access the Administration Tool.
2. Select **Index > Sources and Collections**.
3. In the **Collections** section:
a. Select an existing collection in which you want to add the new source.

OR

b. Click Add to create a new collection.

4. In the Sources section, click Add.

The Add Source page that appears is organized in three sections.

5. In the General Settings section of the Add Source page:

   a. Enter the appropriate value for the following required parameters:

      **Name**

      A descriptive name of your choice for the connector source.

      **Example:** When the source only includes standard Salesforce objects, you could enter: MyCompany Salesforce Organization (Standard Objects)

      **Source Type**

      The connector used by this source. In this case, select Salesforce.
Notes:

- If you do not see **Salesforce** in the **Source Type** list, ensure that your current environment meets the requirements (see "Salesforce Connector Requirements" on page 1448).

- **CES 7.0.5639–(July 2013)** The **Salesforce** item correspond to the source type now identified as **Salesforce (Legacy)**.

Addresses

Enter the Salesforce Website URL: `https://www.salesforce.com/`

Fields

Select the field set that you created for this source (see **Salesforce Connector Deployment Overview**).

Refresh Schedule

Time interval at which the index is automatically refreshed to keep the index content up-to-date. By default, the **Every day** option instructs CES to refresh the source everyday at 12 AM.

The incremental refresh takes care of maintaining the source up-to-date, so you can select a longer interval such as **Every Sunday**. For a CRM Content source, since deleted items cannot be detected by incremental refreshes, you may want to select a shorter interval.

**Tip:** After you create or modify the source configuration, and for each incremental refresh for changed or new items, a Coveo source typically performs the following number of API calls to your Salesforce organization:

- One API call per about 1000 objects
- One API call per attachment
- One API call per about 1000 users
- One API call per group/role/profile/permission sets

With a normal usage, these calls alone will not reach the Salesforce organization daily limit of API calls.

**Note:** You can create new or modify existing source refresh schedules.

b. Review the value for the following parameters that often do not need to be modified:

**Rating**

Change this value only when you want to globally change the rating associated with all items in this source relative to the rating to other sources.

**Example:** When this source indexes a new repository that replaces a legacy repository, you may want to set this parameter to **High**, so that in the search interface, results from this source appear earlier in the list compared to those from the legacy repository.
Document Types

If you defined a custom document type set for this source, select it.

Active Languages

If you defined custom active language sets, ensure to select the most appropriate for this source.

6. In the Specific Connector Parameters & Options section of the Add Source page:

   a. Review the following parameters:

   ObjectsToGet File

   Enter the absolute full path(s) pointing to where you saved the custom ObjectsToGet configuration file(s) that you created (see "Creating a Salesforce ObjectsToGet Configuration File" on page 1472). When you have more than one ObjectsToGet configuration files, separate the full file paths with a semicolon (;) character.

   Note: CES 7.0.6830– (July 2014) The parameter can only contain one path.

   Example:

   D:\CES7\Config\SalesforceObjectsToGet.xml
   ;D:\CES7\Config\SalesforceObjectsToGet2.xml

   Client ID

   Enter the Customer Key value for the Salesforce organization that you want to index (see "Getting Salesforce Client_ID and Client_Secret Values" on page 1453).
Client Secret

Enter the Customer Secret value for the Salesforce organization that you want to index (see "Getting Salesforce Client_ID and Client_Secret Values" on page 1453).

Mapping File

Leave this parameter empty when you want to automatically map all available Salesforce metadata to CES fields using the same name

If you created a mapping file, enter the absolute full path pointing to where you saved the mapping file that you created (see "Creating a Salesforce Mapping File" on page 1505).

Example: D:\CES7\Config\SalesforceMapping.xml

Number of Refresh Threads

When needed, change the number of simultaneous downloads that the connector can handle. The default value is 2.

Sandbox

Select this option only when you want the connector to connect to your Salesforce sandbox (test.salesforce.com) rather than to your Salesforce production environment (login.salesforce.com).

Use Refresh Token

Leave the Use Refresh Token check box cleared unless you want to use the refresh token authentication method. This method is typically used when an application configures the source (such as in the Coveo cloud platform).

b. In the Parameters section, click Add Parameter when you want to show and configure advanced hidden source parameters (see "Modifying Hidden Salesforce Source Parameters" on page 1543).

c. In the Option section, the state of check boxes generally does not need to be changed:

Index Subfolders

Keep this check box selected (recommended). By doing so, all subfolders from the specified starting address are indexed.

Index the document's metadata

When selected, CES indexes all the document metadata, even metadata that are not associated with a field. The orphan metadata are added to the body of the document so that they can be searched using free text queries.

When cleared (default), only the values of system and custom fields that have the Free Text Queries attribute selected will be searchable without using a field query.
Example: A document has two metadata:

- LastEditedBy containing the value Hector Smith
- Department containing the value RH

In CES, the custom field CorpDepartment is bound to the metadata Department and its Free Text Queries attribute is selected.

When the Index the document's metadata option is cleared, searching for RH returns the document because a field is indexing this value. Searching for hector does not return the document because no field is indexing this value.

When the Index the document's metadata option is selected, searching for hector also returns the document because CES indexed orphan metadata.

Document's addresses are case-sensitive

Leave the check box cleared. This parameter needs to be checked only in rare cases for systems in which distinct documents may have the same name but different casing.

Generate a cached HTML version of indexed documents

When you select this check box (recommended), at indexing time, CES creates HTML versions of indexed documents. In the search interfaces, users can then more rapidly review the content by clicking the Quick View link rather than opening the original document with the original application.

Consider clearing this check box only when you do not want to use Quick View links or to save resources when building the source.

Open results with cached version

Leave this check box cleared (recommended) so that in the search interfaces, the main search result link opens the original document in Salesforce.

Consider selecting this check box only when you do not want users to be able to open the original document but only see the HTML version of the document as a Quick View. In this case, you must also select Generate a cached HTML version of indexed documents.

7. In the Security section of the Add Source page:
a. In the **Security Provider** drop-down list:

   **Note:** The selected security provider must have the same values as this source for the **Client ID**, **Client Secret**, and **Sandbox** parameters.

   i. For standard objects and fields and CRM Content sources, select the security provider that you created for this source (see "Configuring a Salesforce Security Provider" on page 1534).

   ii. For a Knowledge Base source, since KB article permissions are not supported, select (none) (see Unsupported Security Aspects).

b. In the **Authentication** drop-down list, select the Salesforce user identity that you created for this source.

c. Click **Save** to save the source configuration.

8. When the source is for secured Salesforce Knowledge Base articles, you have to add permissions at the source level:

   **Important:** The connector does not yet support KB article permissions. This means that, in the Coveo search interface, a user searching Salesforce Knowledge Base content could see content to which he has normally no access in Salesforce.

   **Note:** When your Salesforce Knowledge Base content is not public, a workaround is to enter the name of user(s) or group(s) you want to allow or deny access to your organization content in the **Allowed Users** and **Deny Users** boxes.

   a. In the navigation panel on the left, click **Permissions**.

   b. In the **Permissions** page, select **Specify the security permissions** to index.

   c. In the **Allowed Users** and **Denied Users** boxes, enter the users and groups that you respectively want to allow or deny to see search results from this source. The default is to allow everyone \S-1-1-0\ (Active Directory Group).

   d. Click **Apply Changes**.

9. Rebuild the source.

10. Validate that the source building process is executed without errors:

    - In the navigation panel on the left, click **Status**, and then validate that the indexing proceeds without errors.

    OR

    - Open the CES Console to monitor the source building activities.

What's Next?

Set an incremental refresh schedule for your source.

If you encounter issues:
Solve typical issues that return error messages (see "Troubleshooting Salesforce Connector Issues" on page 1546).

- Consider adding and modifying default values of hidden source parameters (see "Modifying Hidden Salesforce Source Parameters" on page 1543).

9.38.11.1 Modifying Hidden Salesforce Source Parameters

The Add Source and Source: ... General pages of the Administration Tool present the parameters with which you can configure the connector for most Salesforce setups. More advanced and more rarely used parameters are hidden. You can choose to make one or more of these parameters appear in the Add Source and Source: ... General pages of the Administration Tool so that you can change their default value. Consider changing values of hidden parameters only when you encounter time out error messages or performance issues.

The following list describes the available advanced hidden parameters for Salesforce sources. The parameter type (integer, string...) appears between parentheses following the parameter name.

**ExtractPrivateObjectsSharingPermissions (Boolean)** CES 7.0.6684+ (May 2014)

Whether to retrieve and index sharing permissions of private objects. The default is true, in which case when the UseNewPermissionModel parameter is also set to true, for a document with sharing permissions, you can see from the Index Browser a permission model with two levels for share permissions where the second level is READ ACCESS & SHARING for sharing permissions.

**IndexArchivedActivities (Boolean)**

Whether the connector should index archived activities (tasks and events). The default value is False.

**IndexSharingSettings (Boolean)**

Whether to retrieve and index content documents sharing settings. The default value is True.

Indexing sharing settings require one API call per Salesforce record. When indexing sharing permissions is not important for your Salesforce organization, you can turn this option off to save API calls.

**FetchContentVersionOnFeedComments (Boolean)** CES 7.0.8225+ (March 2016)

When indexing Chatter comments, whether to retrieve and index ContentVersion objects on FeedComments. The default value is false. Set to true, when you want to link attachments to the Feed comments in which they appear. In such case, the attachment metadata is added to the related comment field(s).

**LoadFiscalYearMetadata (Boolean)**

Whether the connector should query the Salesforce API to add metadata about fiscal year information. The default value is True.
The fiscal period metadata is available when the Fiscal Year feature is enabled in Salesforce (see How do I set Fiscal Year and start month?).

The following table describes additional fiscal period metadata that will be added for every DateTime metadata that is already available on the item (ex.: if the item contains 2 metadata of type DateTime, then 8 new metadata will be added on the item).

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
<th>Sample Name</th>
<th>Sample Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>id</td>
<td>The unique identifier for a given item. Every item in Salesforce has a unique ID.</td>
<td>id</td>
<td>70130000000rz4C</td>
</tr>
<tr>
<td>{ORIGINAL_METADATA_NAME}__fiscal_year</td>
<td>Contains the fiscal year of the period that includes the date of the {ORIGINAL_METADATA_NAME} metadata.</td>
<td>MyDateField__fiscal_year</td>
<td>2012</td>
</tr>
<tr>
<td>{ORIGINAL_METADATA_NAME}__fiscal_quarter</td>
<td>Contains the fiscal quarter number of the period that includes the date of the {ORIGINAL_METADATA_NAME} metadata.</td>
<td>MyDateField__fiscal_quarter</td>
<td>2</td>
</tr>
<tr>
<td>{ORIGINAL_METADATA_NAME}__fiscal_month</td>
<td>Contains the fiscal month number of the period that includes the date of the {ORIGINAL_METADATA_NAME} metadata.</td>
<td>MyDateField__fiscal_month</td>
<td>20</td>
</tr>
<tr>
<td>{ORIGINAL_METADATA_NAME}__fiscal_week</td>
<td>Contains the fiscal week number of the period that includes the date of the {ORIGINAL_METADATA_NAME} metadata.</td>
<td>MyDateField__fiscal_week</td>
<td>42</td>
</tr>
<tr>
<td>{ORIGINAL_METADATA_NAME}__fiscalquarter</td>
<td>Contains the fiscal quarter in the format {YEAR}-Q(QQUARTER) of the {ORIGINAL_METADATA_NAME} metadata.</td>
<td>MyDateField__fiscalpretty_quarter</td>
<td>2014-Q1</td>
</tr>
</tbody>
</table>

LoginServer (String) CES 7.0.6684+ (May 2014)

The URL of the server you use to log in to your Salesforce organization. The default value is login.salesforce.com. Change the default value when you configure a custom domain and thus disable the ability for your users to log in from login.salesforce.com.

**Note:** You get the following error when the connector cannot log in from the Salesforce login page:

Error with ID 'SALESFORCE_UNABLE_TO_AUTHENTICATE': Failed to connect to the login service.
PrefetchObjectDescriptions (Boolean)

Whether to prefetch object descriptions or not. The default value is true. Prefetching object descriptions often minimizes the number of API calls made to your Salesforce organization, but may sometimes increase the number of calls (see “Minimizing API Calls and Object Description Prefetching” on page 1501).

The formula to determine the optimal value for the PrefetchObjectDescriptions parameter is:

\[
\text{PrefetchObjectDescriptions} = \frac{\text{ObjectsToGet.Objects.Count} - \text{Organization.Objects.Count}}{200}
\]

TimeoutInSeconds (String)

The timeout value for requests made to Salesforce, in seconds. The default value is 600 seconds.

UseConnectorHelpers (Boolean) [CES 7.0.6607+ (April 2014)]

The Coveo Salesforce connector needs to access some information from the Salesforce Metadata API to properly index Salesforce item permissions. Currently, Salesforce requires a very high level of privileges for a user to be able to access this API, even in a read-only manner. The optional Coveo Connector Helpers Package provides an additional API that the connector can use to retrieve the needed information without a high-privilege user (see Using the Coveo Connector Helpers Package).

With the Coveo Connector Helpers package installed in Salesforce, set the UseConnectorHelpers to true to take advantage of the package. When set to true while the Coveo Connector Helpers Package is not installed, the connector falls back to index Salesforce item permissions by directly accessing the Metadata API. The default value is false.

Use the following procedure only when you want to modify one or more of the above hidden source parameters.

To modify hidden Salesforce source parameters

1. Refer to “Adding an Explicit Connector Parameter” on page 450 to add one or more Salesforce hidden source parameters.

2. For a new Salesforce source, access the Add Source page of the Administration Tool to modify the value of the newly added advanced parameter:
   a. Select Index > Sources and Collections.
   b. Under Collections, select the collection in which you want to add the source.
   c. Under Sources, click Add.
   d. In the Add Source page, edit the newly added advanced parameter value.

3. For an existing Salesforce source, access the Source: ... General page of the Administration Tool to modify the value of the newly added advanced parameter:
   a. Select Index > Sources and Collections.
   b. Under Collections, select the collection containing the source you want to modify.
   c. Under Sources, click the existing Salesforce source in which you want to modify the newly added
advanced parameter.

d. In the Source: ... General page, edit the newly added advanced parameter value.

9.38.12 Troubleshooting Salesforce Connector Issues

You can encounter the following error messages when attempting to index your Salesforce organization. Refer to the proposed solutions to resolve issues.

9.38.12.1 API Security Token Required

Error with ID 'SALESFORCE_UNABLE_TO_AUTHORIZE': Failed to authenticate to Salesforce. Failed to connect to the login service. Raw error: {"error":"invalid_grant","error_description":"authentication failure - Failed: API security token required"}

Failed to authenticate to Salesforce. Failed to connect to the login service. Raw error: {"error":"invalid_grant","error_description":"authentication failure - Failed: API security token required"}

When an application such as the Coveo connector accesses Salesforce through the API, the security token must be appended to the password.

Ensure that you appended the security token to the password in the user identity associated with this source (see Creating a Salesforce User Identity).

9.38.12.2 Expired Access/Refresh Token

Error with ID 'SALESFORCE_UNABLE_TO_AUTHORIZE': Failed to authenticate to Salesforce. Failed to connect to the login service. Raw error: {"error":"invalid_grant","error_description":"expired access/refresh token"}

Failed to authenticate to Salesforce. Failed to connect to the login service. Raw error: {"error":"invalid_grant","error_description":"expired access/refresh token"}

When the security provider and/or source User Refresh Token option is selected, you must supply a valid refresh token.

The refresh token authentication method is not the recommended method. Clear the User Refresh Token to rather use the Security Token method (see "Creating a Salesforce User Identity" on page 1449).

9.38.12.3 Missing ionic.zip File

Error with ID 'SALESFORCE_UNABLE_TO_CONNECT': Could not load file or assembly 'Ionic.Zip, Version=1.9.1.8, Culture=neutral, PublicKeyToken=abcdefad942a3f5c' or one of its dependencies. The system cannot find the file specified.

Could not load file or assembly 'Ionic.Zip, Version=1.9.1.8, Culture=neutral, PublicKeyToken=abcdefad942a3f5c' or one of its dependencies. The system cannot find the file specified.

CES 7.0.5785 (August 2013) The required ionic.zip.dll file is missing. Contact Coveo Support to get a copy of this missing file.
9.39 Salesforce Legacy Connector

**Deprecated**

**Important:**

- The Salesforce Legacy connector is removed from Coveo Enterprise Search 7.0 (CES 7) since the March 2016 release.
- The Legacy connector uses the Winter ’12 API (version 23.0) of Salesforce; and since each Salesforce API version is guaranteed to be supported for three years, it is strongly recommended to migrate your Salesforce Legacy source(s) to one(s) that use(s) the second-generation connector for Salesforce. Contact Coveo Support for assistance.

The Coveo Salesforce Legacy connector allows you to crawl Salesforce content and bring it into the unified index, making it easily searchable by end-users. The legacy connector uses a mapping file that defines the database object signatures as well as the objects and fields to index. You can modify the mapping file to customize the indexed content and easily add new object types and custom fields to optimally index your Salesforce database.

**Note:** The Salesforce Legacy connector is now only available to existing users with a CES instance that originally used this connector. The improved replacement solution is Coveo for Salesforce (see Coveo for Salesforce).

### 9.39.1 Features

**Incremental refresh**

The incremental refresh feature refreshes the content of the index based on the modification date of the objects in the Salesforce environment. If an item is modified, the incremental refresh feature refreshes the item automatically.

**Customizable object mapping**

With the mapping file, you can select which Salesforce objects to index. You can decide to index additional custom Salesforce objects and fields, or remove existing ones by just modifying the mapping file (see “Creating and Using a Custom Salesforce Mapping File for the Legacy Connector” on page 1555).

**Metadata**

All the fields of the retrieved Salesforce objects are indexed as metadata. You can therefore customize CES based on that metadata via custom fields.

### Connector Feature History

<table>
<thead>
<tr>
<th>Coveo Platform version</th>
<th>Date</th>
<th>Features</th>
</tr>
</thead>
<tbody>
<tr>
<td>7.0.5785</td>
<td>August 2013</td>
<td>With the introduction of the second generation Salesforce connector, this connector becomes the Salesforce Legacy connector.</td>
</tr>
</tbody>
</table>
What's Next?

Review the deployment process for the Salesforce legacy connector (see "Salesforce Legacy Connector Deployment Overview" on page 1549).

9.39.2 Determining If Sources Use the Salesforce Legacy Connector

Following the March 2016 release, the Salesforce Legacy connector, which is deprecated since the August 2013 release, will be removed from CES 7. The main reason behind this remove is that the legacy connector uses the Winter ‘12 API (version 23.0), which may no longer be supported since Salesforce guarantees three years support for their APIs (see Metadata API Support Policy).

If you index Salesforce content using the Salesforce Legacy connector, it is thus strongly recommended to now use the second-generation connector for Salesforce (see "Salesforce Connector" on page 1440). Contact Coveo Support for assistance on creating Salesforce sources.

To determine if sources use the Salesforce Legacy connector

1. On the Coveo server, access the Administration Tool.
2. Select Configuration > Connectors.
3. In the Connectors page, select Salesforce (deprecated) (CES 7.0.7814+ (August 2015)) or Salesforce Legacy (CES 7.0.7711– (June 2015)).
4. In the Salesforce (deprecated) Connector or Salesforce Legacy Connector page, next to Used By are listed
the sources (if any) that use the Salesforce Legacy connector.

What's Next?

Create a Salesforce source for each of your Salesforce Legacy source with Coveo Support help.

9.39.3 Salesforce Legacy Connector Deployment Overview

**Deprecated**

The following procedure outlines the steps needed to deploy the Salesforce Legacy connector. The steps indicate the order in which you must perform key CES configurations. When needed, the step refers to a detailed procedure.

**Note:** It is strongly recommended to rather use the second generation Salesforce connector.

To deploy the Salesforce legacy connector

1. Validate that your environment meets the requirements (see "Salesforce Legacy Connector Requirements" on page 1550).
2. Configure the user identity.

   The Coveo legacy connector needs an account to connect to your Salesforce environment and access the entire content that you want to index. Create a CES user identity that contains the credentials of a Salesforce
account that has read access to all the Salesforce content that you want to index (see "Adding a User Identity" on page 420).

3. Optionally customize the default mapping file to adapt the Salesforce content to index (see "About the Default Salesforce Mapping File for the Legacy Connector" on page 1550 and "Creating and Using a Custom Salesforce Mapping File for the Legacy Connector" on page 1555).

4. Configure and index the Salesforce source.

The Coveo legacy connector needs to know details about the Salesforce database to be able to index the desired content (see "Configuring and Indexing a Salesforce Source for the Legacy Connector" on page 1561).

5. Add the out-of-the-box or custom Salesforce search interface to a search hub (see "Adding Search Interfaces to a Search Hub With the .NET Interface Editor" on page 544) and then validate that allowed users can search the Salesforce content.

6. Optionally, if you encounter issues, consider adding and modifying default values of hidden source parameters (see "Modifying Hidden Salesforce Source Parameters for the Legacy Connector" on page 1566).

9.39.4 Salesforce Legacy Connector Requirements

 Deprecated

Your environment must meet the following requirements to be able to use the Coveo legacy connector for Salesforce repositories:

- Coveo license including the Salesforce Legacy connector
  
  Your original Coveo license must have included support for the Salesforce legacy connector to be able to use this connector.

- An active Salesforce account to a Salesforce environment

  This account requires a read permission on all the types of content crawled by the connector.

What's Next?

Create a CES user identity for Salesforce (see "Adding a User Identity" on page 420).

9.39.5 About the Default Salesforce Mapping File for the Legacy Connector

 Deprecated

The Coveo legacy connector for Salesforce embeds an XML mapping file that is appropriate for many Salesforce setups. This default mapping file specifies to index the basic Salesforce database object types and the corresponding fields.

The Salesforce object types indexed with the default mapping file are:

- Account
- Contact
- Lead
9.39.5.1 Managing Permissions

The permissions associated to Salesforce content are incorporated into the unified index. When a user makes a query for Salesforce content, the index knows which content this user has access to and only returns query results for content this specific user has access to.

Using the default mapping file

The default mapping file includes a security binding mapping (<AllowedUsers>) that grants access to all users that are members of the Salesforce Users CES custom security group. This mapping is in the <CommonMapping> section of the mapping file and therefore applies to all indexed Salesforce types of content.

Using a custom mapping file

You can customize the mapping file to implement more specific early-binding security mappings, like creating independent custom security groups for each Salesforce type of content (see "Creating and Using a Custom Salesforce Mapping File for the Legacy Connector" on page 1555).

Example: You may want that only users from your Sales department can search the Opportunity type of Salesforce content and only users from your Customer Support department can search the Case type of Salesforce content.

9.39.5.2 Default Mapping File Content

The following XML code presents the content of the default mapping file.

```xml
<?xml version="1.0" encoding="Windows-1252" ?>
<SalesForce>
  <CommonMapping>
    <Fields>
      <ContentType>binarydata</ContentType>
      <sysssfcreatedby>%[CreatedById.Name]</sysssfcreatedby>
      <sysssfcreatedbyid>%[CreatedById]</sysssfcreatedbyid>
      <sysssfcreateddate>%[CreatedDate]</sysssfcreateddate>
      <sysauthor>%[LastModifiedById.Name]</sysauthor>
      <sysdate>%[SystemModstamp]</sysdate>
      <sysssfownerid>%[OwnerId]</sysssfownerid>
      <sysssfowner>%[OwnerId.Name]</sysssfowner>
    </Fields>
    <AllowedUsers>
      <AllowedUser type="CustomGroup" allowed="true">
```

www.coveo.com
<Name>Salesforce Users</Name>
<Server></Server>
</AllowedUser>
</AllowedUsers>
</CommonMapping>
<Mapping type="Account">
   <Title>%[Name]/Title>
   <Body>%[Name]
Owner: %[OwnerId.Name]
Type: %[Type]
Industry: %[Industry]
Description: %[Description] <Body/>
   <sysfiletype>SFAccount</sysfiletype>
   <syssfbillingstreet>%[BillingStreet]</syssfbillingstreet>
   <syssfbillingcity>%[BillingCity]</syssfbillingcity>
   <syssfbillingstate>%[BillingState]</syssfbillingstate>
   <syssfbillingcountry>%[BillingCountry]</syssfbillingcountry>
   <syssfshippingstreet>%[ShippingStreet]</syssfshippingstreet>
   <syssfshippingcity>%[ShippingCity]</syssfshippingcity>
   <syssfshippingstate>%[ShippingState]</syssfshippingstate>
   <syssfshippingcountry>%[ShippingCountry]</syssfshippingcountry>
   <syssfshippingpostalcode>%[ShippingPostalCode]</syssfshippingpostalcode>
   <sysworkphone>%[Phone]</sysworkphone>
   <syssffax>%[Fax]</syssffax>
   <sysworkemail>%[Email]</sysworkemail>
   <syssffirstname>%[FirstName]</syssffirstname>
   <syssflastname>%[LastName]</syssflastname>
   <syssfstreet>%[MailingStreet]</syssfstreet>
   <syssfcity>%[MailingCity]</syssfcity>
   <syssfstate>%[MailingState]</syssfstate>
   <syssfcountry>%[BillingCountry]</syssfcountry>
   <syssfaccountid>%[AccountId.Name]</syssfaccountid>
  </Fields>
</Mapping>
<Mapping type="Contact">
   <Title>%[FirstName] %[LastName] (%[Title])</Title>
   <Body>%[FirstName] %[LastName]
Title: %[Title]
Account: %[AccountId.Name]
Email: %[Email]
Phone: %[Phone]
Address: %[MailingStreet], %[MailingCity], %[MailingState], %[MailingCountry] <Body/>
   <syssffirstname>%[FirstName]</syssffirstname>
   <syssflastname>%[LastName]</syssflastname>
   <syssfstreet>%[MailingStreet]</syssfstreet>
   <syssfcity>%[MailingCity]</syssfcity>
   <syssfstate>%[MailingState]</syssfstate>
   <syssfcountry>%[MailingCountry]</syssfcountry>
   <syssfaccount>%[AccountId.Name]</syssfaccount>
   <syssfaccountid>%[AccountId]%[AccountId]</syssfaccountid>
  </Fields>
</Mapping>
<Mapping type="Lead">
   <Title>%[Company] %[FirstName] %[LastName]</Title>
   <Body>%[FirstName] %[LastName]
Title: %[Title]
SuppliedName : [%[SuppliedName]
SuppliedPhone : [%[SuppliedPhone]
Type : [%[Type]
Description :
  %[Description]
</Body>
</sysfiletype>SFCase</sysfiletype>
</Fields>
</Mapping>
<Maping type="Event">
  <Fields>
    <Title>%[Subject]</Title>
    <Body>%[Description]</Body>
    <sysfiletype>SFEvent</sysfiletype>
    <sysfduration>%[DurationInMinutes]</sysfduration>
    <sysflocation>%[Location]</sysflocation>
  </Fields>
</Mapping>
<Maping type="Task">
  <Fields>
    <Title>%[Subject]</Title>
    <Body>%[Description]</Body>
    <sysfiletype>SFTask</sysfiletype>
    <sysfstatus>%[Status]</sysfstatus>
    <sysfpriority>%[Priority]</sysfpriority>
  </Fields>
</Mapping>
<Maping type="CaseComment">
  <Fields>
    <Body>%[CommentBody]</Body>
    <sysfiletype>SFCaseComment</sysfiletype>
    <syssfcaseid>%[ParentId]</syssfcaseid>
  </Fields>
</Mapping>
<Maping type="EmailMessage">
  <Fields>
    <Title>%[Subject]</Title>
    <Body>%[TextBody]</Body>
    <sysfiletype>SFEmailMessage</sysfiletype>
    <sysfcaseid>%[ParentId]</sysfcaseid>
    <sysdate>%[MessageDate]</sysdate>
    <sysrecipients>%[ToAddress]</sysrecipients>
    <sysfrom>%[FromAddress]</sysfrom>
    <syscc>%[CcAddress]</syscc>
    <sysbcc>%[BccAddress]</sysbcc>
    <sysconversationsubjectid>%[ParentId]</sysconversationsubjectid>
    <sysmailbox>Salesforce.com</sysmailbox>
  </Fields>
</Mapping>
<Maping type="Document">
  <Fields>
    <filename>%[Name]</filename>
    <body>%[Body]</body>
    <Title>%[Name]</Title>
  </Fields>
</Mapping>
<Maping type="Attachment">
  <Fields>
    <filename>%[Name]</filename>
    <body>%[Body]</body>
    <Title>%[Name]</Title>
  </Fields>
</Mapping>
</SalesForce>
9.39.6 Creating and Using a Custom Salesforce Mapping File for the Legacy Connector

You can create a custom mapping file to modify the behavior of the Salesforce legacy connector to adapt to your Salesforce database.

**Tip:** When you want to index only a subset of Salesforce types that are defined in the default mapping file, you do not have to create a custom mapping file. You can simply specify the Salesforce types to index in the **Mapping Types** field for the Salesforce source (see "Configuring and Indexing a Salesforce Source for the Legacy Connector" on page 1561).

To create and use a custom mapping file

1. Copy the content of the default mapping file (see "About the Default Salesforce Mapping File for the Legacy Connector" on page 1550).

2. Using an administrator account, connect to the Coveo Master server.

3. Using a text editor:
   a. In an empty file, paste the content of the default mapping file.
   b. Edit the content of the mapping file to suit your needs, referring to the following subsections for details on how to modify the file:
      - "Mapping file structure" on page 1556
      - "Mapping child nodes" on page 1556
      - "Mapping security" on page 1556
      - "Mapping local expressions" on page 1558
      - "Mapping foreign expressions" on page 1558
      - "Using external resolvers" on page 1558
   c. Save the custom mapping file on the Coveo Master server.

   **Example:** C:\CES7\Config\SalesforceMappingFile.xml

4. Configure the connector to use the custom mapping file in the Salesforce source:
   - When you create a Salesforce source (see "Configuring and Indexing a Salesforce Source for the Legacy Connector" on page 1561).
   - OR
   - For an existing Salesforce source:
      a. On the Coveo server, access the Administration Tool.
      b. Select **Index > Sources and Collections**.
      c. Under **Collections**, select the collection containing the Salesforce source.
      d. Under **Sources**, select the Salesforce source.
e. In the navigation panel on the left, select **General**.

f. In the **Mapping File** parameter, enter the full path to your custom mapping file.

g. Click **Apply Changes**.

5. Rebuild the source.

### 9.39.6.1 Mapping file structure

The mapping file can be divided into three sections:

- **CommonMapping**: All the settings applied to all the mappings.
- **Mapping**: Individual mappings for each object type to index.

You can add mappings for custom Salesforce types not included in the default mapping file simply by copying and editing a mapping section for an existing type.

- **ExternalResolvers**: When you need to apply a sophisticated mapping, you can specify an external assembly type to call to resolve it.

### 9.39.6.2 Mapping child nodes

#### <Fields>

Fields for this mapping. From this point, you either define a system or custom field:

- **System fields**
  
  System fields can be used directly under the **<fields>** node. They are mapped to an existing system field.
  
  **Example**: The **<uri>** is mapped directly to the system field **URI** for this type.
  
- **Custom fields**
  
  Custom fields can be mapped to a custom metadata name. The metadata is filled with the string content.
  
  **Example**: The **<CustomField name="SFLocation">%[Location]</CustomField>** node maps the field named **Location** on the Salesforce object to the metadata **SFLocation** on the document in the unified index.

#### <AllowedUsers>

- **Type of users**: Windows, CustomGroup, CustomUser, ExternalGroup, ExternalUser, WindowSid
- **Name**: Name of the user
- **Server**: Usually references to the domain

### Mapping security

You can configure the Salesforce legacy connector by adding or removing allowed groups and users to the mapping file for each object types. The permissions are therefore incorporated in the index. Using this method is recommended as CES does not have to fetch the security permissions at query time for each query. However,
security permissions can only be set for each object type. This means that individual objects of the same type will always have the same security permissions.

**Example:** The following mapping code gives to the Windows group Sales from the MyOrganization domain access to all the index types as the CommonMapping section applies to all the indexed mappings.

```xml
<CommonMapping>
  <AllowedUsers>
    <AllowedUser type="Windows" allowed="true">
      <Name>Sales</Name>
      <Server>MyOrganization</Server>
    </AllowedUser>
  </AllowedUsers>
</CommonMapping>
```

You can specify different security permissions for each mapping type by adding an AllowedUsers child node to every mapping node.

**Example:** The following mapping code gives access to the Account type to the CES custom security group Salesforce Account Users from the MyOrganization domain.

```xml
<Mapping type="Account">
  <AllowedUsers>
    <AllowedUser type="CustomGroup" allowed="true">
      <Name>Salesforce Account Users</Name>
      <Server>MyOrganization</Server>
    </AllowedUser>
  </AllowedUsers>
  <Fields>
    <Title>%[Subject]</Title>
    <Body>%[Description]</Body>
    <CustomFields>
      <CustomField name="SFOwner">%[OwnerId.FirstName] %[OwnerId.LastName]</CustomField>
      <CustomField name="SFOwnerID">%[OwnerId]</CustomField>
      <CustomField name="SFStatus">%[Status]</CustomField>
      <CustomField name="SFPriority">%[Priority]</CustomField>
    </CustomFields>
  </Fields>
</Mapping>
```

You can also directly set Active Directory users or groups in the mapping file. This method however requires that you modify the mapping file and rebuild the source each time that you add or remove users or groups.
Example: The following mapping code gives access to the Task type to the Active Directory group Sales from the MyOrganization domain.

```xml
<Mapping type="Tasks">
  <AllowedUsers>
    <AllowedUser type="Windows" allowed="true">
      <Name>Sales</Name>
      <Server>MyOrganization</Server>
    </AllowedUser>
  </AllowedUsers>
  <Fields>
    <Title>%[Subject]</Title>
    <Body>%[Description]</Body>
    <CustomFields>
      <CustomField name="SFOwner">%[OwnerId.FirstName] % [OwnerId.LastName]</CustomField>
      <CustomField name="SFOwnerID">%[OwnerId</CustomField>
      <CustomField name="SFStatus">%[Status]</CustomField>
      <CustomField name="SFPriority">%[Priority]</CustomField>
    </CustomFields>
  </Fields>
</Mapping>
```

9.39.6.3 Mapping local expressions

The Salesforce legacy connector uses a specific mapping expression to represent a value on a Salesforce object. Occurrences of the expression `%%field%%` are replaced by the value of the field specified by the name in the brackets for this Salesforce object.

Example: The expression `<ModifiedDate>%[LastModifiedDate]</ModifiedDate>` replaces the string `% [LastModifiedDate]` by the value of the `LastModifiedDate` field for each Salesforce object. The value fetched is then assigned to the system field `ModifiedDate` on each document in the unified index.

9.39.6.4 Mapping foreign expressions

As some objects can reference to others in Salesforce, you can fetch the value of a foreign field in your mappings, as long as the foreign type has the requested field.

Example: The expression `<CustomField name="SFOwner">%[OwnerId.FirstName] % [OwnerId.LastName]</CustomField>` retrieves the specific object pointed by `OwnerId` and retrieves the value of the fields `FirstName` and `LastName` on that object. Then the resulting string is a concatenation of both results. An example of the result for this expression could be `John Smith`.

Important: Foreign expressions can dramatically slow down the indexing process, as a remote object has to be queried for every foreign expression. Coveo has a local cache for each field value; however the performance decreases every time it has to fetch field values on a new object. Use them carefully.

9.39.6.5 Using external resolvers

When declaring an external resolver, you need to provide a unique name as well as a fully qualified type name to call.

```xml
<SalesForce>
  <ExternalResolvers>
    <ExternalResolver name="Resolvername" type="FQTypename"/>
  </ExternalResolvers>
</SalesForce>
```
Once the external resolver has been defined, you can use it in any mapping using the following syntax: @ [resolvername].

Parameters can be defined to pass to the external type. In this case, you must specify an additional bracket node with parameters separated by a semicolon ():@[resolvername][param1;param2].

As the external resolvers are called last, fields to resolve (such as @ [field]) can be specified as parameters and will be resolved before the external resolver is called.

External resolver type limitations

For the external type to be used with the external resolver system, you must write a DLL that implements the IMappingResolver interface defined as follows:

```csharp
namespace Coveo.CES.CustomCrawlers.SalesForce
{
    /// <summary>
    /// the Interface the callback functions in the mapping file must implement.
    /// </summary>
    public interface IMappingResolver
    {
        string Resolve(string[] p_Parameters,
                        Record p_CurrentRecord,
                        MappingUtilities pUtilities);
    }
}
```

The parameters are passed as an array of string in p_Parameters. The current record being parsed is passed as well as p_CurrentRecord. Finally, the connector cached records, connection, disk cache, etc. can be accessed using the mapping utilities. The string returned by the resolve function will be used as the mapping value.

All these classes and interfaces are in the Salesforce legacy connector assembly, the external assemblies will need to add the Salesforce connector assembly as a reference.

9.39.7 Configuring a Salesforce Security Provider for the Legacy Connector

Deprecated

The Coveo legacy connector needs to resolve mappings between users and groups from your Salesforce environment and Microsoft Active Directory.

Once the security provider is created, you must associate it to the Salesforce source. The security provider is invoked every time a user performs a query and validates with Salesforce if the user performing the query has the right to view each document in the query results. This process can be slow; however it allows individual security permissions for each document instead of having permissions for each object type. Users are required to enter their account information for Salesforce sources in the Search Interface when using this security method.

Note: You can get familiar with how Coveo components deal with permissions on documents both at indexing and query time.
To configure a Salesforce security provider for the legacy connector

1. On the Coveo server, access the Administration Tool.
3. In the Security page, in the navigation panel on the left, click Security Providers.
4. In the Security Providers page, click Add to create a new security provider.
5. In the Modify Security Provider page:

   a. Configure the following required parameters:

   **Name**

   Choose a meaningful name to identify the security provider.

   **Example:** Salesforce Security Provider (Legacy Connector)

   **Security Provider Type**

   In the drop-down list, select **Salesforce (Legacy) (x64)**.

   **Note:** CES 7.0.5639–(July 2013) The Salesforce Legacy connector appears in the list as Salesforce (x64).
User Identity

In the drop-down list, select the user identity that you created for this source.

b. Revise the default value for the following parameters that generally do not need to be changed:

Salesforce Login Url

The URL used to login to Salesforce Web services. The default value is https://login.salesforce.com/.

Salesforce API Version

The API version of Salesforce Web services to connect to, specified in the ##.## format. The default value is 23.0.

Timeout Time

The communication timeout allowed for any request sent to the Salesforce Web services. The default value is 100 seconds.

c. In the Parameters section, in rare cases the Coveo Support could instruct you to click Add Parameters to specify other security provider parameter names and values that could help to troubleshoot security provider issues.

d. Leave the Allow Complex Identities option cleared as it does not apply to this type of security provider.

e. Click Apply Changes.

What's Next?

Create you Salesforce source (see "Configuring and Indexing a Salesforce Source for the Legacy Connector" on page 1561).

9.39.8 Configuring and Indexing a Salesforce Source for the Legacy Connector

Deprecated

A source defines a set of configuration parameters for a specific Salesforce database.

Note: When your organization has access to more than one Salesforce environment, you must define one source for each Salesforce environment that you want to index.

To configure and index a Salesforce source for the legacy connector

1. On the Coveo server, access the Administration Tool.

2. Select Index > Sources and Collections.

3. In the Collections section:
   a. Select an existing collection in which you want to add the new source.

   OR
b. Click **Add** to create a new collection.

4. In the **Sources** section, click **Add**.

   The **Add Source** page that appears is organized in three sections.

5. In the **General Settings** section of the **Add Source** page:

   ![Add Source page](image)

   a. Enter the appropriate value for the following required parameters:

      **Name**

      A descriptive name of your choice for this legacy connector source.

      **Example**: Salesforce site (Legacy connector)

      **Source Type**

      **CES 7.0.7814+ (August 2015)** The connector used by this source. In this case, select **Salesforce** (deprecated).
Notes:

- If you do not see Salesforce (deprecated) in the Source Type list, ensure that your current environment meets the requirements (see “Salesforce Legacy Connector Requirements” on page 1550).

- CES 7.0.7711– (June 2015) The Salesforce Legacy connector appears in the list as Salesforce (Legacy) (x64).

- CES 7.0.5639– (July 2013) The Salesforce Legacy connector appears in the list as Salesforce (x64).

- CES 7.0.5785+ (August 2013) The Salesforce (x64) type corresponds to the source to be used with the second generation Salesforce connector.

Addresses

Enter the Salesforce Website URL: http://www.salesforce.com/

Refresh Schedule

Time interval at which the index is automatically refreshed to keep the index content up-to-date. By default, the Every day option instructs CES to refresh the source everyday at 12 AM.

Note: You can create new or modify existing source refresh schedules.

b. Review the value for the following parameters that often do not need to be modified:

Rating

Change this value only when you want to globally change the rating associated with all items in this source relative to the rating to other sources.

Example: When this source replaces a legacy system, you may want to set this parameter to High, so that in the search interface, results from this source appear earlier in the list compared to those from the source for the legacy system.

Document Types

If you defined a custom document type set for this source, select it.

Active Languages

If you defined custom active language sets, ensure to select the most appropriate for this source.

Fields

If you defined custom field sets, ensure to select the most appropriate for this source.

6. In the Specific Connector Parameters & Options section of the Add Source page:
a. Consider using the following optional parameters:

**Mapping File**

Leave this box empty to use the default mapping file that instructs the connector to index basic Salesforce elements and use the Salesforce Users CES custom security group to manage permissions (see "About the Default Salesforce Mapping File for the Legacy Connector" on page 1550).

When you choose to create a custom mapping file, enter the absolute full path pointing to your custom mapping file (see "Creating and Using a Custom Salesforce Mapping File for the Legacy Connector" on page 1555).

**Example:** C:\CES7\Config\SalesforceMappingFile.xml

**Mapping Types**

Leave this box empty to instruct the connector to index all the mapping types defined in the default or custom mapping file.

This parameter is useful to easily index only a subset of mapping types among the ones defined in the mapping file. Enter each type to index separated by semicolons (see "About the Default Salesforce Mapping File for the Legacy Connector" on page 1550).

**Example:** Enter: Event;Task;Case. The content for the other types will not be indexed.

b. In the **Parameters** section, click **Add Parameter** when you want to show and configure advanced hidden source parameters (see "Modifying Hidden Salesforce Source Parameters for the Legacy Connector" on page 1566).

c. In the **Option** section, the state of check boxes generally does not need to be changed:

**Index Subfolders**

Keep this check box selected (recommended). By doing so, all subfolders from the specified starting address are indexed.

**Index the document's metadata**

When selected, CES indexes all the document metadata, even metadata that are not associated with a
field. The orphan metadata are added to the body of the document so that they can be searched using free text queries.

When cleared (default), only the values of system and custom fields that have the Free Text Queries attribute selected will be searchable without using a field query.

**Example:** A document has two metadata:

- #LastEditedBy containing the value Hector Smith
- Department containing the value RH

In CES, the custom field CorpDepartment is bound to the metadata Department and its Free Text Queries attribute is selected.

When the Index the document's metadata option is cleared, searching for RH returns the document because a field is indexing this value. Searching for hector does not return the document because no field is indexing this value.

When the Index the document's metadata option is selected, searching for hector also returns the document because CES indexed orphan metadata.

**Document's addresses are case-sensitive**

Leave the check box cleared. This parameter needs to be checked only in rare cases for systems in which distinct documents may have the same name but different casing.

**Generate a cached HTML version of indexed documents**

When you select this check box (recommended), at indexing time, CES creates HTML versions of indexed documents. In the search interfaces, users can then more rapidly review the content by clicking the Quick View link rather than opening the original document with the original application. Consider clearing this check box only when you do not want to use Quick View links or to save resources when building the source.

**Open results with cached version**

Leave this check box cleared (recommended) so that in the search interfaces, the main search result link opens the original document with the original application. Consider selecting this check box only when you do not want users to be able to open the original document but only see the HTML version of the document as a Quick View. In this case, you must also select Generate a cached HTML version of indexed documents.

7. In the Security section of the Add Source page:
a. In the **Security Provider** drop-down list, select the security provider that you created for this source (see "Configuring a Salesforce Security Provider for the Legacy Connector" on page 1559).

b. In the **Authentication** drop-down list, select the Salesforce user identity that you created.

c. Click **Save and Start** to save the source configuration and start indexing this source.

8. Validate that the source building process is executed without errors:

   - In the navigation panel on the left, click **Status**, and then validate that the indexing proceeds without errors.

   OR

   - Open the CES Console to monitor the source building activities.

What's Next?

Set an incremental refresh schedule for your source.

9.39.9 Modifying Hidden Salesforce Source Parameters for the Legacy Connector

**Deprecated**

The **Add Source** and **Source: ... General** pages of the Administration Tool present the parameters with which you can configure the legacy connector for most Salesforce setups. More advanced and more rarely used parameters are hidden. You can choose to make one or more of these parameters appear in the **Add Source** and **Source: ... General** pages of the Administration Tool so that you can change their default value. Consider changing values of hidden parameters only when you encounter time out error messages or performance issues.

**Note:** The Salesforce legacy connector uses the open connector framework and can therefore be modified using custom parameters such as `liveindexingdelay` (see Connector API Home).

The following list describes the available advanced hidden parameters for Salesforce sources. The parameter type (integer, string,...) appears between parentheses following the parameter name.

**Timeout (String)**

The communication timeout allowed for any request sent to the Salesforce Web services. The default value is 100 seconds.
NbRefreshThreads (string)

The number of threads used to handle the indexing operation of the Salesforce repository. The default value is 1.

FilterExpression (string)

The list of conditions to add to any query sent to Salesforce. These conditions are appended to the WHERE clause of the Salesforce Object Query Language (SOQL) statement sent via the Web services. There is no default value.

Example: ParentId='5007000000JQpLnAAL' indexes all items that have the specified parent ID.

CustomLoginUri (string)

The URI used to login to Salesforce Web services. The default value is https://login.salesforce.com/.

CustomLoginUriVersion (string)

The API version of Salesforce Web services to connect to, specified in the ##.# format. The default value is 23.0.

CustomBaseUri (string)

The base URI used for indexed documents. In other words, this forces the Uri and ClickableUri properties to have the specified base URI. The default value is https://na1.salesforce.com/.

FixXmlNamespace (Boolean)

Whether empty XML namespaces received in Web service responses must be fixed before processing. The default value is False.

QueryLimit (Integer)

The maximum number of results returned by a query to Salesforce. The default value is 5000 items.

QueryBatchSize (Integer)

The maximum number of results contained in a query result object (QueryMore). The default value is 200 items.

ForeignCacheSize (Integer)

The B-tree cache size used by the foreign cache. The default value is 3145728 bytes.

ForeignPageSize (Integer)

The B-tree page size used by the foreign cache. The default value is 65536 bytes.

PrefetchCacheSize (Integer)

The B-tree cache size used by the prefetch cache. The default value is 1000 items.

ExcludeConvertedLeads (Boolean)

When True, leads that are converted will not be indexed. The default value is True.
ExcludeDeletedItems (Boolean)

When True, items that are marked as "IsDeleted" will not be indexed. The default value is True.

Use the following procedure only when you want to modify one or more of the above hidden source parameters.

To modify hidden Salesforce source parameters

1. Refer to "Adding an Explicit Connector Parameter" on page 450 to add one or more Salesforce hidden source parameters.

2. For a new Salesforce source, access the Add Source page of the Administration Tool to modify the value of the newly added advanced parameter:
   a. Select Index > Sources and Collections.
   b. Under Collections, select the collection in which you want to add the source.
   c. Under Sources, click Add.
   d. In the Add Source page, edit the newly added advanced parameter value.

3. For an existing Salesforce source, access the Source: ... General page of the Administration Tool to modify the value of the newly added advanced parameter:
   a. Select Index > Sources and Collections.
   b. Under Collections, select the collection containing the source you want to modify.
   c. Under Sources, click the existing Salesforce source in which you want to modify the newly added advanced parameter.
   d. In the Source: ... General page, edit the newly added advanced parameter value.

9.40 Sitemap Connector

CES 7.0.7599+ (April 2015)

The Sitemap connector allows you to index listed web pages from a Sitemap (Sitemap file or a Sitemaps index file). For secured websites (non-public accessible Sitemap), the connector supports some authentication modes.

9.40.1 Connector Features Summary

<table>
<thead>
<tr>
<th>Features</th>
<th>Supported</th>
<th>Additional information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sitemap version</td>
<td>XML, Text, RSS 2.0, and Atom 1.0</td>
<td>Sitemap files and Sitemap index file must respect the Sitemap protocol (validations can however be turned off by a parameter)</td>
</tr>
<tr>
<td>Searchable content type</td>
<td>✔</td>
<td>Web pages (URL)</td>
</tr>
</tbody>
</table>
Features | Supported | Additional information
---|---|---
Content update | Incremental refresh | ✓ | Full refresh or rebuild needed to retrieve deleted web pages and text sitemap changes. Requires the Sitemap to define the optional Last Modification Date attribute (e.g., `<lastmod>` for XML Sitemaps, `<updated>` for Atom Sitemaps, `<pubDate>` for RSS Sitemaps) for each URL to be supported. (missing or bad snippet) The Last Modification Date attribute must specify the modification time in the W3C DateTime format: `YYYY-MM-DDThh:mm:ss`.  
| Full refresh | ✓ |  
| Rebuild | ✓ |  
| Document-level security | ✗ | Permissions must be manually defined on the source [more]  

9.40.2 Features

The features of the Sitemap connector are:

**Content indexing**

The connector can retrieve and index exclusively web pages from Sitemaps:

**Supported Sitemap file formats**

The connector can retrieve web pages from the following Sitemap file formats (see [Sitemap protocol](#)):  
- XML (Sitemap and index)  
  
  **Note:** CES 7.0.7814+ (August 2015) Support sitemap files containing custom metadata (see "Adding and Indexing Custom Metadata in an XML Sitemap" on page 1583).  
- Text  
- Syndication Feeds (Atom 1.0 and RSS 2.0)  
- HTML CES 7.0.7711+ (June 2015)

**Supported authentication schemes**

The connector can authenticate with the following authentication schemes:

- Basic  
- Digest  
- NTLM


- Negotiate/Kerberos
- Form-based CES 7.0.7914+ (October 2015)

### Incremental refresh

Periodically queries your Sitemap for the latest items modifications (addition, edition), keeping the index content up-to-date.

#### Notes:
- The Sitemap must define the optional Last Modification Date attribute (e.g., `<lastmod>` for XML Sitemaps, `<updated>` for Atom Sitemaps, `<pubDate>` for RSS Sitemaps) for each URL. If not, you need to perform a source full refresh to catch changes. Text Sitemaps do not contain this attribute.
- Deleted web pages require a full refresh to be taken in account.

### Pause/Resume

When indexing Sitemap content, the connector can be paused and resumed.

### 9.40.3 Sitemap Connector Deployment Overview

The following procedure outlines the steps needed to deploy the Sitemap connector. The steps indicate the order in which you must perform configuration tasks on the Coveo server.

To deploy the Sitemap connector

1. Validate that your environment meets the requirements (see "Sitemap Connector Requirements" on page 1570).

2. On the Coveo server, in the Coveo Administration Tool:
   a. When you have an authentication on your website, create a user identity (see "Adding a User Identity" on page 420).
   b. Create a Sitemap field set to take advantage of the available Sitemap metadata.
      i. It is recommended to start by importing the default Sitemap field set file ([CES\Path]\Bin\Coveo.CES.CustomCrawlers.Sitemap.FieldSet.xml) to create fields for all the metadata available by default from sitemaps.
      ii. When you created custom metadata for your Sitemap documents, add corresponding fields to the field set.
   c. Configure and index a Sitemap source.
      The connector must know details about the Sitemap file or Sitemap index to index their content (see "Configuring and Indexing a Sitemap Source" on page 1571).
   d. If you encounter issues, verify if modifying the default value of hidden source parameters can help resolve the problems (see "Modifying Hidden Sitemap Source Parameters" on page 1579).

### 9.40.4 Sitemap Connector Requirements

Your environment must meet the following requirements to be able to use the Sitemap connector:
Coveo license for the Sitemap connector

Your Coveo license must include support for the Sitemap connector to be able to use this connector.

What's Next?

Review the deployment process (see "Sitemap Connector Deployment Overview" on page 1570).

9.40.5 Configuring and Indexing a Sitemap Source

A source defines a set of configuration parameters for one or more Sitemap files listing the content of your site.

To configure and index a source with the Sitemap connector

1. On the Coveo server, access the Administration Tool.

2. Select Index > Sources and Collections.

3. In the Collections section:
   a. Select an existing collection in which you want to add the new source.
   OR
   b. Click Add to create a new collection.

4. In the Sources section, click Add.

5. In the General Settings section of the Add Source page:

   General Settings
   - Name: My Organization Website Sitemap
   - Source Type: Sitemap
   - Addresses: http://myorganization.com/baseweb/websiteindex.xml
   - Rating: Normal
   - Document Types: Default
   - Active Languages: Default
   - Fields: Sitemap Field set
   - Refresh Schedule: Everyday
a. Enter the appropriate value for the following required parameters:

Name

Enter a descriptive name of your choice for the connector source.

**Example:** My Organization Website Sitemap

Source Type

The connector used by this source. In this case, select *Sitemap*.

Addresses

Enter the URLs to one or more Sitemap files or Sitemap index files in either the http:// or https:// form.
Notes:

- By default, Sitemap files and Sitemap index files that do not respect the following validations based on the Sitemap protocol are ignored during the indexing process (see Sitemap protocol):
  - An uncompressed Sitemap file must be no larger than 10 MB (even if the file is compressed with GZIP).
  - A Sitemap file cannot contain more than 50,000 URLs.
  - All referenced URLs must be less than 2,048 characters.
  - All referenced URLs must be relative to the Sitemap that references them and in the same domain. The location of a Sitemap file determines the set of URLs that can be included in that Sitemap.

  **Example:** A Sitemap file located at http://myorgwebsite.com/tech/sitemap.xml can include any URLs starting with http://myorgwebsite.com/tech/ but cannot include URLs starting with http://myorgwebsite/catalog/.

- When you do not want your Sitemap files and Sitemap index files to be validated, add the `ParseSitemapInStrictMode hidden parameter with the false value` (see Modifying Hidden Sitemap Source Parameters). In this case, the above validations are not performed. Consequently, all web pages are indexed if their reference URL is valid and absolute.

- When you want to retrieve the content of listed web pages from a XML Sitemap, enter the direct Sitemap URL instead of the Sitemap website address. Otherwise, the source could interpret the web page as a Sitemap file in HTML and crawl the discovered links.

  **Example:** You enter the following URL: http://myorgwebsite.com/sitemap.xml instead of http://myorgwebsite.com/.

- The Sitemap connector can retrieve all links contained in a web page. The Sitemap crawler does not expand all discovered links, but only crawls the web page as a Sitemap file in HTML.

  You can also select only a specific part of a web page to be indexed by adding the `HtmlXPathSelectorExpression hidden parameter. The parameter value must be an XPath expression that selects one or more nodes of a web page containing the URLs to crawl (see Modifying Hidden Sitemap Source Parameters). By default, the connector indexes all listed web pages from an HTML Sitemap.

  **Example:** You want only to index a specific portion (only the web pages linked inside the cbc-sitemap div container) of the CBC Sitemap web page, so you add the parameter with the following value: //div[@id='cbc-sitemap'].

  - Any XPath selecting node can be used to set the website portion to include (see XPath syntax).
- You should also set the `ParseSitemapInStrictMode` hidden parameter to `false` since an HTML web page does not follow the Sitemap protocol (see Sitemap Protocol).

Examples:

- `http://myorgwebsite.com/sitemap.xml` (Public website Sitemap)
- `http://myorgwebsite.com/sitemap.xml.gz` (Public website Sitemap compressed with GZIP)
- `http://myorgwebsite.com/sitemap` (Web page containing links such as a site map)

You can enter more than one Sitemap file or Sitemaps index file address on separate lines, but you must ensure that all source parameters apply to all Sitemap files. Otherwise, create other sources.

Refresh Schedule

Time interval at which the index is automatically refreshed to keep the index content up-to-date. By default, the **Every day** option instructs CES to refresh the source everyday at 12 AM.

b. Review the value for the following parameters that often do not need to be modified:

**Rating**

Change this value only when you want to globally change the rating associated with all items in this source relative to the rating to other sources.

**Example:** If this source was for an important Sitemap, you may want to set this parameter to **High**, so that in the search interface, results from this source appear earlier in the search result list compared to those from other sources.

**Document Types**

If you defined custom document type sets, ensure to select the most appropriate for this source.

**Active Languages**

If you defined custom language sets, ensure to select the most appropriate for this source.

**Fields**

Select the field set that you created earlier (see Sitemap Connector Deployment Overview).

6. In the **Specific Connector Parameters & Options** section of the **Add Source** page:
Specific Connector Parameters & Options

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Number of Refresh Threads</td>
<td>2</td>
</tr>
<tr>
<td>Mapping File</td>
<td>Coveo.CES.CustomCrawlers.Sitemap.xml</td>
</tr>
<tr>
<td>User-agent HTTP header</td>
<td>Mozilla/5.0 (Windows NT 6.1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/27.0.1453.110 Safari/537.36</td>
</tr>
</tbody>
</table>

a. Review if you need to change the default values for the following parameters:

**Number of Refresh Threads**

Determines the number of refresh threads that allow the connector to crawl web pages in parallel. The default value is 2 threads.

**Notes:**

- **CES 7.0.8047+ (December 2015)** The connector supports multiple threads (2+) for websites that use a form-based authentication.
- **CES 7.0.7914 (October 2015)** You must set the value to 1.
- Increasing this value may improve source refresh speed but puts more load on the website server.

**Mapping File**

The path to the mapping file. Leave the default value to use the default mapping file that comes with the connector (Coveo.CES.CustomCrawlers.Sitemap.MappingFile.xml). If you create a custom mapping file, enter the full path to your custom mapping file. Contact Coveo Support for assistance if you need to customize the mapping file.

**User-Agent HTTP header**

Determines the identifier used by the Sitemap connector to identify itself when downloading web pages. The default value is Mozilla/5.0 (Windows NT 6.1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/27.0.1453.110 Safari/537.36.

b. In the **Parameters** section, click **Add Parameter** to be able to change the default value of hidden parameters (see "Modifying Hidden Sitemap Source Parameters" on page 1579).
Notes:

- **CES 7.0.8225+ (March 2016)** (For XML sitemaps only) When the last modification dates are not in a standard format (ex: YYYY-MM-DDThh:mm:ss.sTZD), thus triggering an error in the CES Console (SITEMAP_INVALID_FORMAT_ERROR with an Invalid date), add the DateFormat hidden parameter to specify the Sitemap file date custom format. The format must use the MSDN format specifiers (see Custom Date and Time Format Strings and DateFormat).

  Example: yyyy:MM:ddTHH:mm:sszzz

- **CES 7.0.7814+ (August 2015)** When you use basic authentication and you get an HTML 404 error in the CES Console, you can add the ForceBasicAuthorizationHeader hidden parameter and set it to true (see ForceBasicAuthorizationHeader).

c. In the Option section, review the default value of the following check boxes:

  **Index subfolders**

  This option, a generic connector parameter, is not taken into account and has no effect for the Sitemap connector.

  **Index the document’s metadata**

  When selected, CES indexes all the document metadata, even metadata that are not associated with a field. The orphan metadata are added to the body of the document so that they can be searched using free text queries.

  When cleared (default), only the values of system and custom fields that have the Free Text Queries attribute selected will be searchable without using a field query.

  Example: A document has two metadata:

  - LastEditedBy containing the value Hector Smith
  - Department containing the value RH

  In CES, the custom field CorpDepartment is bound to the metadata Department and its Free Text Queries attribute is selected.

  When the **Index the document’s metadata** option is cleared, searching for RH returns the document because a field is indexing this value. Searching for hector does not return the document because no field is indexing this value.

  When the **Index the document’s metadata** option is selected, searching for hector also returns the document because CES indexed orphan metadata.

  **Generate a cached HTML version of indexed documents**

  When you select this check box (recommended), at indexing time, CES creates HTML versions of indexed documents. In the search interfaces, users can then more rapidly review the content by clicking the Quick View link rather than opening the original document with the original application. Consider clearing this check box only if you do not want to use Quick View links or to save resources when building the source.
Open results with cached version

Leave this check box cleared (recommended) so that in the search interfaces, the main search result link opens the original document with the original application. Consider selecting this check box only when you do not want users to be able to open the original document but only see the HTML version of the document as a Quick View. In this case, you must also select Generate a cached HTML version of indexed documents.

7. When you have an authentication on your website, in the Security section of the Add Source page:

![Security Section]

a. In the Authentication drop-down list, select the Sitemap user identity that you created for this source (see Sitemap Connector Deployment Overview). Otherwise, select (none).

Note: By specifying a User Identity, the connector can authenticate using the following supported authentication schemes:

- Basic
- Digest
- NTLM
- Negotiate/Kerberos
- Form-based [CES 7.0.7914+ (October 2015)]

Some setups can be problematic, but most of the setups should be supported. You can use the ManualCookies hidden parameter when your website does not use one of these authentication schemes (see Modifying Hidden Sitemap Source Parameters).

b. Click Save and Start to save the source configuration and build the source.

8. Manually set the security on the source, by changing the default Permissions option to set the permissions globally on the source:

Note: You get the following error message in the CES Console when the Index security permissions option is selected by default:

Permissions indexing is not provided by the Sitemap connector. You must manually configure the permissions on the source.

a. In the navigation panel on the left, select Permissions.

b. In the Permissions page:
i. Select the **Specifies the security permissions to index** option.

ii. Optionally, in the **Allowed Users** list, add or remove users or groups to precisely specify who has access to the content from this source.

   By default, the Active Directory `everyone \S-1-1-0\` group specifies that any Active Directory user can see all the content from this source.

iii. Optionally, in the **Denied Users** list, add users or groups to specify who has not access to the content from this source.

iv. Click **Apply Changes**.

9. On the toolbar, click **Start/Rebuild** to start indexing your source.

10. Validate that the source building process is executed without errors:

    a. In the navigation panel on the left, click **Status**, and then validate that the indexing proceeds without errors.

    OR

    b. Open the CES Console to monitor the source building activities.

What's Next?

Set an incremental refresh schedule for your source.
9.40.5.1 Modifying Hidden Sitemap Source Parameters

The **Add Source** and **Source: ... General** pages of the Administration Tool present the parameters with which you can configure the connector for most Sitemap setups. More advanced and more rarely used parameters are hidden. You can choose to make one or more of these parameters appear in the **Add Source** and **Source: ... General** pages of the Administration Tool so that you can change their default value. Consider changing values of hidden parameters when you encounter issues.

The following list describes the advanced hidden parameters available with Sitemap sources. The parameter type (integer, string, etc.) appears between parentheses following the parameter name.

**IndexHtmlMetadata (Boolean) CES 7.0.8541+ (September 2016)**

Whether metadata tags found in HTML files should be indexed. The `content` attribute of `meta` tags is indexed when the tag is keyed with one of the following attributes: `name`, `property`, `itemprop`, or `http-equiv`. The default value is `false` since the parameter has an impact on indexing performance.

**Example:** In the tag `<meta property="og:title" content="The Article Title"/>`, **The Article Title is indexed.**

**AdditionalWebRequestHeaders (String)**

Semicolon separated list of additional HTTP headers added to the connector requests in the following format: `key1=value1;key2=value2`.

**Date Format (String) CES 7.0.8225+ (March 2016)**

(For XML sitemaps only) When the last modification dates are not in a standard format (ex: `YYYY-MM-DDThh:mm:ss.sTZD`), thus triggering an error in the CES Console (SITEMAP_INVALID_DATE_FORMAT_ERROR with an Invalid date), specify the Sitemap file date custom format. The format must use the MSDN format specifiers (see Custom Date and Time Format Strings).

**Example:** `yyyy;MM;ddHH:mm:sszzz`

**FormAuthConfigurationPath (String) CES 7.0.7914+ (October 2015)**

The path to the form-based authentication XML configuration file.

**Note:** The **UseCookies** hidden parameter must be set to `true`. If not, you get the following warning during your sitemap source rebuild:

Ensure the username and password are valid and that you are supplying all the values submitted by the form at "{0}". The request to authenticate did not support HTTP cookies but the authentication form set the following cookies: {0}. This may have caused the form authentication to fail. Consider turning on HTTP cookies support.

**ForceBasicAuthorizationHeader (Integer) CES 7.0.7814+ (August 2015)**

Whether to force basic authentication header in the web request without waiting the server challenge. The default value is `false`. Set it to `true` when your server does not challenge the caller for authentication for example or when you get an HTTP 404 error (often occurs on non-IIS servers) in the CES Console that looks like the following:
Exception during item expansion: https://myorgwebsite.com/basicauth/user/password. -->
The remote server returned an error: (404) Not Found.

ParseSitemapInStrictMode (Boolean)

Whether each Sitemap file should be parsed in strict mode or not. When the Sitemap file does not follow the protocol specification (see Protocol Standard Validations), the parsing throws an exception. The default value is false. Set to true when you want to index your Sitemap files with protocol standard validations.

Note: CES 7.0.7914–(October 2015) The default value was true.

ReadTimeout (Integer)

The timeout duration in seconds when the connector reads web page content from a stream (i.e., downloading a Sitemap/web page content). The default value is 300 seconds.

Timeout (Integer)

The number of seconds to wait before the request (i.e., server responding to a request) times out. The default value is 100 seconds.

AllowAutoRedirect (Boolean)

Whether the request should automatically follow redirection responses from the web resource or not. The default value is true.

NumberOfRetries (Boolean)

The number of retries allowed when a failed web request is recoverable. Only the following HTTP errors will be retried: 408, 500 and 503. The default value is 3 retries.

UseCookies (Boolean)

Whether cookies must be enabled to crawl. The default value is false. Set the value to true when you want a cookie container to be initialized and reused for each web request for the crawling.

ManualCookies (String)

A collection of manual cookies to inject with each HTTP web request in the following format:

MyCookieName=MyCookieValue;Domain=coveo.com;Expires=Wdy, DD Mon YYYY HH:MM:SS GMT;Path=/;Domain=mydomain.com;Secure;HttpOnly

where you need to enter your information at the specified places.

When you need to define more than one cookie, separate each cookie definition with the ;; separator. The default value is null. Use this parameter when your website does not use one of the four supported authentication schemes and thus needs a specific cookie to be used for crawling (see Supported Authentication Schemes).

Example:

MyFirstCookie=MyFirstValue;Domain=www.coveo.com;;MySecondCookie=MySecondValue;Domain=www.example.com
Notes:

- The only mandatory attributes are the cookie name, its value and the domain (where the cookie belongs to). All attributes must be separated using a semicolon (;) character.

- The supported optional attributes are:
  - Expires: the expiration date in RFC 1123 format (Wdy, DD Mon YYYY HH:MM:SS GMT);
  - Path: the subfolder path where the cookie belongs to (relative to the root domain);
  - Secure: means to keep cookie communication limited to encrypted transmission;
  - HttpOnly: directs browsers to not expose cookies through channels other than HTTP (and HTTPS) requests.

The Secure and HttpOnly attributes do not have associated values. The presence of their attribute names indicates that their behaviors are enabled.

HtmlXPathSelectorExpression (String) CES 7.0.7711+ (June 2015)

The XPath expression used to select one or more nodes in an HTML document containing the URLs to crawl. By default, the connector indexes all listed web pages from an HTML Sitemap.

Example: You only want to index a specific portion (only the web pages linked inside the cbc-sitemap div container) of the CBC Sitemap web page so you add the parameter with the following value: //div[@id='cbc-sitemap'].

Notes:

- The ParseSitemapInStrictMode hidden parameter should be set to false since an HTML web page does not follow the Sitemap protocol (see Sitemap Protocol).

- Any XPath selecting nodes can be used to set the website portion to index (see XPath Syntax).

ScrapingConfiguration (String) CES 7.0.8541+ (September 2016)

The JSON web scraping configuration that allows you to specify CSS or XPATH selectors to:

- Filter pages.
- Exclude page sections.

Example: Exclude page sections such as the header, the footer, or a side panel that are similar in all pages and are considered noise in the index.

- Scrap metadata from pages.

Example: Extract to a metadata a blog post publication date string that is only available in a specific div in the page (not in a meta tag). You can then map the metadata to a field that can be used in the blog search result template so search user can easily identify when the blog was published.
This option adds useful flexibility to the Sitemap connector. The JSON configuration syntax is the same as the one used in Coveo Cloud V2 Web or Sitemap sources (see Web Scraping Configuration).

When you add the hidden parameter, simply paste the appropriate valid JSON configuration in the parameter value box.

![Screen capture showing the JSON configuration syntax example](image)

**Note:** The Sitemap connector does not support the sub-item web scraping feature, allowing to split a crawled page in more than one index item. If you do include such configuration, it will simply be ignored.

### EnableJavaScript (Boolean) CES 7.0.8541+ (September 2016)

Whether the JavaScript should be evaluated and rendered before the indexation. The default value is `false`. This option is useful when you want to index the dynamically rendered content of crawled pages. Be aware however that activating this option has a significant impact on the crawling performance.

### IndexHtmlMetadata (Boolean) CES 7.0.8541+ (September 2016)

Whether the metadata tags found in HTML files should be scrapped and passed to the index. The feature extracts the `content` attribute value for all `meta` HTML elements with a `name`, `property`, `itemprop`, or `http-equiv` attribute as well as the `title` HTML element value. The default value is `false`.

**Notes:**

- Enabling this option may significantly reduce the crawling performance as the crawler must scrap each page.
- The CES converter by default also more efficiently extracts `meta` HTML elements with a `name` attribute. Consider enabling this option only when you want to extract `meta` HTML elements with a `property`, `itemprop`, or `http-equiv` attribute.

To modify hidden Sitemap source parameters

1. Refer to "Adding an Explicit Connector Parameter" on page 450 to add one or more Sitemap source parameters.

2. For a new Sitemap source, access the Add Source page of the Administration Tool to modify the value of the newly added advanced parameter:
   a. Select **Index > Sources and Collections**.
   b. Under **Collections**, select the collection in which you want to add the source.
c. Under Sources, click Add.

d. In the Add Source page, edit the newly added advanced parameter value.

3. For an existing Sitemap source, access the Source: ... General page of the Administration Tool to modify the value of the newly added advanced parameter:
   a. Select Index > Sources and Collections.
   b. Under Collections, select the collection containing the source you want to modify.
   c. Under Sources, click the existing Sitemap source in which you want to modify the newly added advanced parameter.
   d. In the Source: ... General page, edit the newly added advanced parameter value.

4. Rebuild your Sitemap source to apply the changes to the parameters.

9.40.6 Adding and Indexing Custom Metadata in an XML Sitemap

**CES 7.0.7814+ (August 2015)**

The Sitemap connector now supports to index Coveo specific custom metadata that a developer adds to an XML sitemap file. When a developer can generate or modify the sitemap XML file of a repository to index, he can also include a Coveo namespace (coveo:metatada) and metadata to provide information on documents that is not found in the out-of-the-box fields (Sitemap field set and Coveo System fields).

**Example:** Since you have control on the sitemap file (not a third party that generates it), you decide to create your XML sitemap file dynamically and add all the custom metadata you need.

The added Coveo metadata will only be read by the Coveo crawler and connector but ignored by all other processes, but respect the Sitemap protocol (see Sitemap protocol).

The following procedure requires a user that has the permissions and skills to modify or create an XML sitemap file and access to the CES Administration Tool.

To add and index custom metadata in an XML Sitemap

1. You or a developer must code a third-party process to modify or create an XML sitemap file as follows:

   **Note:** Contact Coveo Professional Services if you need assistance.

   a. In the urlset XML element start tag (<urlset>), extend the Sitemap protocol using the Coveo namespace by adding the following line:

```
<urlset
    xmlns:coveo="http://www.coveo.com/schemas/metadata"
```

**Example:**

```
<?xml version="1.0" encoding="UTF-8"?>
<urlset
    xmlns="http://www.sitemaps.org/schemas/sitemap/0.9"
    xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
    xsi:schemaLocation="http://www.sitemaps.org/schemas/sitemap/0.9
http://www.sitemaps.org/schemas/sitemap/0.9/sitemap.xsd"
    xmlns:coveo="http://www.coveo.com/schemas/metadata">
```
b. For each `<url>` element in the sitemap, create a new XML element named `coveo:metadata` (`<coveo:metadata></coveo:metadata>`).

Example:
```
<url>
  <loc>http://example.com/about/</loc>
  <lastmod>2015-02-10T13:47:23+00:00</lastmod>
  <changefreq>weekly</changefreq>
  <priority>1.00</priority>
  <coveo:metadata>
    <modificationdate>2015-02-10T13:47:23+00:00</modificationdate>
  </coveo:metadata>
</url>
```

c. Within the `coveo:metadata` elements, add your custom metadata (name and value).

Notes: CES 7.0.8850+ (March 2017)
- Character Data (CDATA) is supported when you place the CDATA tag (`<![CDATA[]]`) at the beginning of the node (see Character Data and Markup).

Example:
```
<coveo:metadata>
  <casenumber>18467</casenumber>
  <companyname>
    <![CDATA[
      Company XYZ Inc. <USA>
    ]]>)
  </companyname>
</coveo:metadata>
```
- The connector ignores the CDATA tag and indexes the rest of the node content such as special characters (e.g., `, %, $, and ~) and `<xml>` tags as text.

Example: You want to add the name of the author, the last date of modification and the document tags (if any) so you add the following XML elements:
```
<coveo:metadata>
  <modificationdate>2015-02-10T13:47:23+00:00</modificationdate>
  <authorname>John Smith</authorname>
  <tags />
</coveo:metadata>
```

Once done, the sitemap could look like the following:
```
<?xml version="1.0" encoding="UTF-8"?>
<urlset
  xmlns="http://www.sitemaps.org/schemas/sitemap/0.9"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  xsi:schemaLocation="http://www.sitemaps.org/schemas/sitemap/0.9 http://www.sitemaps.org/schemas/sitemap/0.9/sitemap.xsd"
  xmlns:coveo="http://www.coveo.com/schemas/metadata">
  <url>
    <loc>http://example.com/about/</loc>
    <lastmod>2015-02-10T13:47:23+00:00</lastmod>
    <changefreq>weekly</changefreq>
    <priority>1.00</priority>
    <coveo:metadata>
      <modificationdate>2015-02-10T13:47:23+00:00</modificationdate>
    </coveo:metadata>
  </url>
</urlset>
```
2. In the Administration Tool, for the custom metadata you want to see in your document details, add the corresponding custom fields with the `sitemap` prefix in the sitemap field set (see "Adding or Modifying Custom Fields" on page 494).

**Note:** It is not mandatory to add every custom metadata, but when you do so the **Name** must match the XML element name.

**Important:** XML element names are case-sensitive.

**Example:** You want to have the author name in the results metadata so you add the `sitemapauthorname` field.

3. Build or rebuild your Sitemap source.

4. In the Index Browser, verify that the new metadata are available on your Sitemap source documents.

### 9.41 Symantec Enterprise Vault Connector

The Symantec Enterprise Vault (SEV) connector allows to crawl most of the data contained within the different archives of a SEV system, most notably Windows files and Microsoft Exchange items.

The Coveo Platform provides a more efficient search than the SEV built-in search component and offers the possibility to search in live and archived data at the same time.

#### 9.41.1 Features

The following details the features available in the SEV connector:
Archive targets

Supported:

- Windows File system
- Microsoft Exchange Server

Limited support:

- SharePoint: Available data limited to what SEV stores.

Not supported:

- Lotus Notes

Security

The Coveo Platform indexes SEV stored permissions. SEV stores permissions at the folder level only.

Incremental refresh

Allows incremental indexing to reduce index, SEV, and network resources.

Metadata

- Uri: Uses the same scheme as the Starting Addresses.
- PrintableUri: Original location of the file (kvsOriginalLocation).
- ClickableUri: Points SEV Web server to view Vault files (msg)kvsBrowserViewURL.
- ModifiedDate
- Author

- sysAuthor, kvsArhiveld, kvsSaveSetId, kvsCreatedDate, kvsFileExtension, kvsMIMEFormat, kvsModifiedDate, kvsOriginalLocation, kvsOriginalSize, kvsDefaultMSGFormat

9.41.2 Feature history

<table>
<thead>
<tr>
<th>CES version</th>
<th>Date</th>
<th>Features</th>
</tr>
</thead>
<tbody>
<tr>
<td>7.0.8691+</td>
<td>December 2016</td>
<td>Veritas Enterprise Vault version 12 support</td>
</tr>
<tr>
<td>7.0.6942+</td>
<td>August 2014</td>
<td>Symantec Enterprise Vault version 11 support</td>
</tr>
<tr>
<td>7.0.4855+</td>
<td>August 2012</td>
<td>Symantec Enterprise Vault version 10 support</td>
</tr>
</tbody>
</table>

9.41.3 Symantec Enterprise Vault Connector Deployment Overview

The following procedure outlines the steps needed to deploy the Symantec Enterprise Vault connector. The steps indicate the order in which you must perform key CES configurations. When needed, the step refers to a detailed procedure.
1. Validate that your environment meets the requirements (see "Symantec Enterprise Vault Connector Requirements" on page 1587).

2. For a Symantec Enterprise Vault version 10 server, you must enable the indexing service (see "Enabling Symantec Enterprise Vault Services" on page 1588).

3. Configure the user identity.

   The Coveo connector needs an account to connect to your Symantec Enterprise Vault environment. Create a CES user identity (see "Adding a User Identity" on page 420) that contains the credentials of a Symantec Enterprise Vault account that meets the following requirements:

   a. Read access to the archives to index (see Granting Permission to All Archives).
   b. Read access to the SQL Server database called enterprisevaultdirectory.
   c. Member of the Local Administrators Group on the Enterprise Vault server

   OR

   - Create a new user which is a copy of the Service Account user in Enterprise Vault. This user should already have access to the database and all mailboxes.

4. Configure and index the Symantec Enterprise Vault source.

   The Coveo connector needs to know details about the Symantec Enterprise Vault system to be able to index the desired content (see "Configuring and Indexing a Symantec Enterprise Vault Source" on page 1590).

5. Optionally, if you encounter issues, consider adding and modifying default values of hidden source parameters (see "Modifying Hidden Symantec Enterprise Vault Source Parameters" on page 1595).

9.41.4 Symantec Enterprise Vault Connector Requirements

Your environment must meet the following requirements to be able to use the Coveo connector for Symantec Enterprise Vault (SEV) systems:

- Coveo license that includes support for the SEV connector
- SEV versions:
  - Supported versions: 10, 11, 12
  - Depreciated support versions: 7, 8
- SEV directory, indexing, and storage services must be running (see "Enabling Symantec Enterprise Vault Services" on page 1588).
- SEV Administration Console component installed on the Coveo Master server
9.41.5 Enabling Symantec Enterprise Vault Services

The following services must be running on your Symantec Enterprise Vault (SEV) server to allow the Coveo connector for SEV to work:

- Enterprise Vault Directory Service (allows the connector to discover archives)
- Enterprise Vault Indexing Service (allows the connector to enumerate archive items)
- Enterprise Vault Storage Service (allows the connector to retrieve item content)

In SEV 9 and earlier, these services are enabled by default. In SEV 10, the Enterprise Vault Indexing Service is not running by default and must be configured and started.

To enable the Enterprise Vault Indexing Service for SEV 10

1. Using an administrator account, connect to your Enterprise Vault 10 server.

2. In the Enterprise Vault console, in the panel on the left, under Enterprise Vault Servers, right-click your server, and then select Properties.

3. In the Computer Properties dialog box:
   a. Select the Cache tab.
   b. In the Cache settings section, in the Cache location box, browse or enter the path for the cache and then
4. Back in the **Enterprise Vault**, in the panel on the left, under your server, click **Services**.

5. In the panel on the right, right-click **Enterprise Vault Indexing Service**, select **Start**, and then ensure that its **Status** turns to **Running**.
9.41.6 Impersonating a Symantec Enterprise Vault User

Impersonation is performed when a user connects to Symantec Enterprise Vault (SEV) using a different identity than the one used to run CES.

**Note:** The Windows firewall and possibly other firewalls can sometimes cause severe performance issues with the SEV connector. Calls that should return in less than a second may take more than the default connector timeout value of 30 seconds and prevent getting any documents. You must configure or turn off the firewall to avoid these issues.

To connect to SEV using impersonation

1. On the Coveo Master server, promote the user being impersonated to Administrator.
2. In the firewall settings (including Windows Firewall if it is used), enable the [CES_Paths]\Bin\Coveo.CNL.HostProcess.exe process.

9.41.7 Configuring and Indexing a Symantec Enterprise Vault Source

A source defines a set of configuration parameters for a Symantec Enterprise Vault (SEV) system.

To configure and index a SEV source

1. On the Coveo server, access the Administration Tool.
2. Select Index > Sources and Collections.
3. In the Collections section:
a. Select an existing collection in which you want to add the new source.

OR

b. Click Add to create a new collection.

4. In the Sources section, click Add.

The Add Source page that appears is organized in three sections.

5. In the General Settings section of the Add Source page:

![General Settings](image)

a. Enter the appropriate value for the following required parameters:

Name

A descriptive name of your choice for the connector source.

Example: Symantec Enterprise Vault

Source Type

The connector used by this source. In this case, select Symantec Enterprise Vault.

Note: If you do not see SaleSymantec Enterprise VaultsForce in the Source Type list, ensure that your current environment meets the requirements (see “Symantec Enterprise Vault Connector Requirements” on page 1587).
Addresses

The list of SEV starting points to crawl, one entry per line. Specify addresses in the form Server>site>store>archive where > is the path separator.

Examples: To index a whole store: serverName>siteName>storeName
To index only an archive in a store: serverName>siteName>storeName>archiveName

Refresh Schedule

Time interval at which the source is automatically refreshed to keep the index content up-to-date. By default, the Every day option instructs CES to refresh the source everyday at 12 AM.

Note: You can create new or modify existing source refresh schedules.

b. Review the value for the following parameters that often do not need to be modified:

Rating

Change this value only when you want to globally change the ranking associated with all items in this source relative to the rating of other sources.

Example: Because this source contains archived content, you may want to select Low, so that in the search interface, results from this source appear later in the list compared to those from other sources.

Document Types

If you defined custom document type sets, ensure to select the most appropriate for this source.

Active Languages

If you defined custom active language sets, ensure to select the most appropriate for this source.

Fields

If you defined custom field sets, ensure to select the most appropriate for this source.

6. In the Specific Connector Parameters & Options section of the Add Source page:
a. Configure the following required parameters:

**SQL Server Host Name**

Name of the machine hosting the SQL server and database containing the security information for the SEV on which the user is connected.

**Connection String**

Connection string to the SQL database (for System.Data.SqlClient: db name, db server connection security parameters, etc.).

**Examples:**

- **Standard security:**
  
  Data Source=myServerAddress;Initial Catalog=myDataBase;User Id=myUsername;Password=myPassword;

- **Standard security alternative syntax that produces the same result:**
  
  Server=myServerAddress;Database=myDataBase;User ID=myUsername;Password=myPassword;Trusted_Connection=False;

- **Trusted connection:**
  
  Data Source=myServerAddress;Initial Catalog=myDataBase;Integrated Security=SSPI;

- **Trusted connection alternative syntax that produces the same result:**
  
  Server=myServerAddress;Database=myDataBase;Trusted_Connection=True;

Use the serverName\instanceName form for Data Source to use a specific SQL Server instance.

**Note:** The multiple SQL Server instances feature is available only from SQL Server version 2000+. 


Number of Refresh Threads

Determines the number of threads that are querying SEV for data. The default and recommended value is 1. More threads speed up the crawling process, but increase the server load.

Database Name

The name of your SEV administration database. The default value is EnterpriseVaultDirectory.

Index EV Securities for Mailbox Archives

For archives of mailbox type, select this option to combine the permissions found in the SEV database with the permissions found on the mailbox in Active Directory. The default value is False.

b. In the Option section, the state of check boxes generally does not need to be changed:

Index Subfolders

Check to index all subfolders below the specified starting addresses. This option is selected by default.

Index the document’s metadata

When selected, CES indexes all the document metadata, even metadata that are not associated with a field. The orphan metadata are added to the body of the document so that they can be searched using free text queries.

When cleared (default), only the values of system and custom fields that have the Free Text Queries attribute selected will be searchable without using a field query.

Example: A document has two metadata:

- LastEditedBy containing the value Hector Smith
- Department containing the value RH

In CES, the custom field CorpDepartment is bound to the metadata Department and its Free Text Queries attribute is selected.

When the Index the document’s metadata option is cleared, searching for RH returns the document because a field is indexing this value. Searching for hector does not return the document because no field is indexing this value.

When the Index the document’s metadata option is selected, searching for hector also returns the document because CES indexed orphan metadata.

Document’s addresses are case-sensitive

Leave the check box cleared. This parameter needs to be checked only in rare cases for case sensitive systems in which distinct documents may have the same file name but with different casing.

Generate a cached HTML version of indexed documents

When you select this check box (recommended), at indexing time CES creates HTML versions of indexed documents and saves them in the unified index. In the search interfaces, users can then more rapidly review the content by clicking the Quick View link to open the HTML version of the item rather
than opening the original document with the original application.

Consider clearing this check box only if you do not want to use Quick View links or to save resources when building the source.

**Open results with cached version**

Leave this check box cleared (recommended) so that in the search interfaces, the main search result link opens the original document with the original application. Consider selecting this check box only when you do not want users to be able to open the original document but only see the HTML version of the document as a Quick View. When this option is selected, you must also select the **Generate a cached HTML version of indexed documents** check box.

7. In the **Security** section of the **Add Source** page:

   ![Security section of the Add Source page](image)

   a. In the **Active Directory Security Provider** drop-down list, select **Active Directory** or a custom Active Directory security provider that you created for a specific domain.

   b. In the **Authentication** drop-down list, select the Symantec Enterprise Vault user identity that you created.

   c. Click **Save and Start** to save the source configuration and start indexing this source.

8. Validate that the source building process is executed without errors:

   - In the navigation panel on the left, click **Status**, and then validate that the indexing proceeds without errors.

     OR

   - Open the CES Console to monitor the source building activities.

**What’s Next?**

Set an incremental refresh schedule for your source.

9.41.8 Modifying Hidden Symantec Enterprise Vault Source Parameters

The **Add Source** and **Source: ... General** pages of the Administration Tool present the parameters with which you can configure the connector for most setups. More advanced and more rarely used parameters are hidden.

You can choose to make one or more of these parameters appear in the **Add Source** and **Source: ... General** pages of the Administration Tool so that you can change their default value. Consider changing values of hidden parameters only when you encounter time out error messages or performance issues.
The available advanced hidden parameters for Symantec Enterprise Vault (SEV) sources are presented in the following list with the parameter type (integer, string…) appearing between parentheses following the parameter name.

**IgnoreArchiveSecurities (Boolean)**

Set this option to True to ignore the security parameters found on the archive and only use the item permissions. The default value is False.

**LowerBoundDate (String)**

This parameter defines the lowest modification date of items that will be indexed. Modifying this parameter requires a source refresh.

Example: When you need to index a SEV that contains a large amount of data over several years, crawling the whole content may take days or even weeks. You can use the LowerBoundDate and UpperBoundDate parameters to create sources for specific periods and start indexing the sources for the most recent periods first.

**UpperBoundDate (String)**

This parameter defines the highest modification date of items that will be indexed. Modifying this parameter requires a source refresh.

**LDAPSearchRoot (String)**

Specifies to the connector where to start looking in Active Directory. When this parameter is not specified, the connector looks at the root of Active Directory, which can be extremely large. By specifying a value, you can refine the search.

Example: To search only within the organizational unit (OU) companynameOU within the domain corp.companyname.com, enter:

LDAP://OU=companynameOU, DC=corp, DC=companyname, DC=com

**LDAPFilters (String)**

Filter applied to the search of Active Directory in order to find mailboxes. Allows adding properties to the results the connector is looking for. The default filter is: (& (mail=*) (objectclass=user) (objectclass=person)).

This AND operation is performed on a few properties to find the maximum number of mailboxes without receiving any unwanted ones. If this filter is not specific enough, you can complete the filter by adding a value to the AND operation on the filter.

Example: When you enter the value cn=JohnSmith in the parameter, the resulting filter is: (& (mail=*) (objectclass=user) (objectclass=person) (cn=JohnSmith))

**EnforceADSecurities (Boolean)**

When set to True, all archived mailboxes that do not have Active Directory (AD) permissions are rejected and not crawled. When set to False, a warning appears in the log about the lack of permissions. The default value is False.
MaxNumberOfRetries (Integer)

The number of attempts to make when performing an action on SEV. The default value is \(3\).

RetryDelay (Integer)

The amount of time to wait between SEV action retry attempts, in seconds. The default value is \(30\).

TimeOut (Integer)

The amount of time given to perform a request to Active Directory, in seconds. For file downloads, it is the amount of time with no progress before aborting the operation. The default value is \(30\).

BatchSize (Integer)

The number of documents IDs to pre-fetch per request before downloading them. The default value is \(100\).

Use the following procedure only when you want to modify the above hidden source parameters.

To modify hidden source parameters

1. Refer to "Adding an Explicit Connector Parameter" on page 450 to add a hidden source parameter.

2. For a new source, access the Add Source page of the Administration Tool to modify the value of the newly added advanced parameter:
   a. Select Index > Sources and Collections.
   b. Under Collections, select the collection in which you want to add the source.
   c. Under Sources, click Add.
   d. In the Add Source page, edit the newly added advanced parameter value.

3. For an existing source, access the Source: ... General page of the Administration Tool to modify the value of the newly added advanced parameter:
   a. Select Index > Sources and Collections.
   b. Under Collections, select the collection containing the source you want to modify.
   c. Under Sources, click the existing source in which you want to modify the newly added advanced parameter.
   d. In the Source: ... General page, edit the newly added advanced parameter value, and then click Apply Changes.
9.42 Twitter v2 Connector

Twitter is an online social networking service that enables users to post and read short messages called "Tweets". Registered users can post and read Tweets; unregistered users can only read them. The second generation (v2) of the Coveo connector for Twitter allows Coveo administrators to index and integrate the Twitter content of their managed users into a Coveo unified index. The connector indexes specific content from all managed users, so that any user can easily find the Twitter content he has access rights to through any Coveo search interface.

9.42.1 Features

The Twitter v2 connector features:

**Content indexing**

- Extraction and indexing of the following Twitter item types:
  - Users
  - Usernames and names
  - Protected users (see Limitations)
  - Tweets (normal, mention, reply, retweets, quote)
  - Hashtags (#) and cashtags ($)
  - Symbols
  - Timelines (user, home, mentions, lists, collections)
  - Lists
  - Collections

**Incremental refresh**

Supports incremental refresh to periodically query Twitter for the latest Tweets, newly followed users and newly listed members, keeping index content up-to-date.

*Note: Some changes need a full refresh or a source rebuild to be taken into account (see Limitations).*

**Multi-threading**

Can run multiple threads, which can improve performances considerably (see Configuring and Indexing a Twitter v2 Source).

**Pause/Resume**

When indexing Twitter content, connector tasks can be paused and resumed.
9.42.2 Limitations

- The connector does not support permissions. Permissions need to be defined manually.
- A Twitter API limitation prevents the connector from supporting user mappings.
- During an incremental refresh, deleted items cannot be detected and require a full refresh or rebuild to be updated or removed.
- Incremental refresh cannot be performed if the last rebuild or refresh did not end normally, i.e., the source was stopped, paused, or an exception occurred.
- Direct messages are not indexed.
- Tweets belonging to protected users (protected Tweets) cannot be retrieved from a search query.

**Note:** Protected Tweets can only be retrieved from a user timeline if the authenticated user is an approved follower of the protected user.

What's Next?

Review the steps to deploy the Twitter v2 connector (see "Twitter v2 Connector Deployment Overview" on page 2).

9.42.3 Twitter v2 Connector Deployment Overview

The following procedure outlines the steps needed to deploy the Twitter v2 connector. The steps indicate the order in which you must perform configuration tasks on both the Twitter and Coveo servers.

To deploy the Twitter v2 connector

1. Validate that your environment meets the requirements (see "Twitter v2 Connector Requirements" on page 2).
2. From the Twitter server, obtain the necessary API, token, and secret access codes (see "Obtaining the Twitter API and Access Token" on page 3).
3. On the Coveo server, in the Coveo Enterprise Search (CES) Administration Tool:
   a. Configure and index a Twitter v2 source.
      - The connector must know certain details to access and index the Twitter content of your managed users (see "Configuring and Indexing a Twitter v2 Source" on page 5).
   b. Fine tune connector performance by modifying (if necessary) the default value of hidden source parameters. This step also applies if you encounter indexing issues (see "Modifying Hidden Twitter v2 Source Parameters" on page 12).

9.42.4 Twitter v2 Connector Requirements

For you to use the Twitter v2 connector, your environment must meet the following requirements:

- **CES 7.0.8388+ (June 2016)**
- Coveo license for the Twitter v2 connector

Your Coveo license must include support for the Twitter v2 connector to be able to use this connector.
• A valid Twitter user account
• An active corporate Twitter application

Notes:
- It is strongly suggested that you generate your Twitter account access token upon creation of your account. Doing this will simplify various operations requiring the use of API keys and access tokens.
- It is considered a best practice to setup a Twitter application dedicated to the Coveo connector.

What's Next?
Grant Coveo access to the valid Twitter account and, in turn, to the content of all your managed users (see Obtaining the Twitter API and Access Token).

9.42.5 Obtaining the Twitter API and Access Token
The following procedure outlines the steps needed to obtain the values given by your Twitter application when configuring a Twitter v2 source to index.

To obtain the API and Access Token values
1. From any browser, sign in your Twitter application.

2. Click on the name of your application and, on the screen that appears, log in with your username and password.
3. In the **Application Management** screen, click **Keys and Access Tokens** under your application name.

   On the page that appears, under **Application Settings**, you will find the application **Consumer Key (API Key)** and **Consumer Secret (API Secret)**, and under **Your Access Token**, you will find the application **Access Token** and **Access Token Secret**.

4. Stay on this page until you have input these keys and tokens in the appropriate fields when configuring the Twitter v2 connector in the Administration Tool (see Configuring and Indexing a Twitter v2 Source).
What's Next?

Configure and start indexing Twitter accounts and, in turn, the Twitter content of all your managed users (see 9.4.2.6 Configuring and Indexing a Twitter v2 Source).

9.4.2.6 Configuring and Indexing a Twitter v2 Source

A source defines a set of configuration parameters for a specific Twitter account.

To configure and index a Twitter v2 source

1. On the Coveo server, access the Administration Tool.
2. Select Index > Sources and Collections.
3. In the Collections section:
- Select an existing collection to which you want to add the new source.

  OR

- Click Add to create a new collection.

4. In the Sources section, click Add.

The Add Source page that appears is organized in two sections.

5. In the General Settings section of the Add Source page:

![Add Source Page](image)

   a. Enter the appropriate value for the following required parameters:

      Name
      Enter a descriptive name of your choice for the connector source.

      Example: Twitter v2

      Source Type
      Select the connector used by this source. In this case, select Twitter v2.

      Note: If you do not see Twitter v2, your environment does not meet the requirements (see “Twitter v2 Connector Requirements” on page 2).

      Addresses
      Starting addresses are source locations in your Twitter account. The Twitter v2 connector supports four
types of starting addresses. Enter all required starting addresses:

- **users**: a list of comma-separated usernames.
  
  **Example**: users:twitterapi,coveo,support

- **list**: a list's name and its creator's username in the format (username)/(listname). These values can be obtained in the list's URL (https://twitter.com/{username}/lists/{listname}).
  
  **Example**: list:twitterapi/meetup-20100301

- **query**: a search query. Only Tweets posted within the last 7 days will be retrieved with this starting address, and the results are not comprehensive (some Tweets posted in the last week might be missing).
  
  **Examples**:
  - query:#coveo
  - query:$GE
  - query:puppy filter:media

- **collection**: a collection's ID, which can be obtained from the collection's URL (https://twitter.com/{username}/timelines/{ID}).
  
  **Example**: collection:719516944244817923

b. Review the value for the following and seldom-modified parameters:

**Rating**

Change this value only when you want to globally change the rating associated with this source relative to the rating of other sources.

**Example**: When a source replaces a legacy system, you may want to set this parameter to **High** so that, in the search interface, results from this source appear higher in the list compared to those from legacy system sources.

**Document Types**

If you defined a custom document type set for this source, select it.

**Active Languages**

If you defined custom active language sets, make sure that you select the most appropriate for this source.

**Fields**

Coveo Enterprise Search (CES) 7.0 does not require the presence of custom field sets to extract metadata from Twitter. However, if you elected to use a specific field set, you can select it in the **Fields** drop-down list. Otherwise, leave it at **Default Scheme**.
Refresh Schedule

Time interval at which index content is automatically updated. By default, the Every day option instructs CES to refresh the source every day at 12 AM. Since the incremental refresh takes care of updating the source, you can select a longer interval such as Every Sunday.

Note: Since deleted items are not taken into account during normal incremental refresh operations (see "Limitations" on page 2), it is recommended to force a full refresh, or even a source rebuild, to update the status of those deleted items.

6. In the Specific Connector Parameters & Options section of the Add Source page:

![Specific Connector Parameters & Options](image)

a. Enter the previously obtained values. These values allow the Twitter v2 connector to access the content of your managed Twitter users.

Note: These values are long series of alphanumeric characters.

API Key

The API key provides the identity of your corporate Twitter application when crawling the data of managed Twitter users whose Twitter account needs to be indexed.
API Secret

The API secret is used to authenticate the API key above.

Access Token

The access token is used to make API requests on behalf of your corporate Twitter application.

Note: This access token is used to retrieve a new OAuth 1.0a access token.

Access Token Secret

The access token secret is used to authenticate the access token above.

b. The default value for the following parameters often does not need to be changed:

Number of refresh threads

Determines the number of threads that the connector can refresh simultaneously. The default and recommended value is 2.

Mapping File

Indicates the path to the default mapping file that defines how the connector handles metadata. The installer creates the file indicated is this field.

c. Select additional content to be indexed using the following options:

Index User’s Followings

Indexes the Tweets of users that a managed user is following. With this check box selected, users followed by users specified in users:user1,user2,... starting addresses will be retrieved. By default, this check box is not selected.

Index Mentions

Indexes the Tweets mentioning a user specified in a users:user1,user2... starting address. By default, this check box is not selected.

Note: Only Tweets from the last 7 days will be indexed. Mention Tweets are retrieved by searching for "@username", so parameters set for search query results will also affect the mention Tweets retrieved.

Example: if SearchResultIsoLanguageCode is set to "fr", only mention Tweets written in French will be retrieved.

Index Retweets

Indexes all retweets when retrieving Tweets from a user timeline. By default, this check box is selected.

Index Replies

Indexes all replies when retrieving Tweets from a user timeline. By default, this check box is selected.
Note: When the Index Retweets and Index Replies check boxes are not selected, the number of Tweets retrieved per page will be up to the number specified with the TweetsPerTimelinePage parameter, because results are filtered after being retrieved.

Keep old items

With this check box selected, items are not deleted, even if they are not recrawled. By default, this check box is selected. Items are not deleted unless this check box is cleared.

Note: Old items can be removed by manually removing a folder or an item from the index, clearing this check box or deleting the source.

d. (Optional) Click Add Parameter when you want to show and change the value of advanced source parameters (see "Modifying Hidden Twitter v2 Source Parameters" on page 12).

e. The Option check boxes generally do not need to be changed:

Index Subfolders

When selected, CES indexes subfolders recursively. By default, this check box is selected.

Index the document’s metadata

When selected, CES indexes all the document metadata, even metadata that is not associated with a field. Orphan metadata is added to the body of the document so that it can be searched using free text queries.

When this check box is cleared (default), only system and custom field values for which the Free Text Queries attribute is selected will be searchable without using a field query.

Example: A document has the following metadata:

- LastEditedBy containing the value Hector Smith
- Department containing the value RH

In CES, the custom field CorpDepartment is bound to the metadata Department and its Free Text Queries attribute is selected.

When the Index the document’s metadata option is cleared, searching for RH returns the document because a field is indexing this value. Searching for hector does not return the document because no field is indexing this value.

When the Index the document’s metadata option is selected, searching for hector also returns the document because CES indexed orphan metadata.

Document’s addresses are case-sensitive

Determines if, when two addresses differ only by their casing, they are considered as two different addresses. This check box is cleared by default.

Generate a cached HTML version of indexed documents

At indexing time, CES creates HTML versions of indexed documents. In search interfaces, users can
then more quickly review the content by clicking the Quick View link rather than opening the original document with the original application. By default, this check box is selected. Consider clearing this check box only when you neither want to use Quick View links nor save resources when indexing the source.

**Open results with cached version**

Leave this check box cleared (recommended) so that, in search interfaces, the main search result link opens the original document with the original application. Consider selecting this check box only when you do not want users to be able to open the original document but only see the HTML version of the document as a Quick View. In this case, you must also select **Generate a cached HTML version of indexed documents**.

7. Click **Save** to save the source configuration. You are brought back to the **Source** page.

8. In the Permissions section of the Source page, select **Specifies the security permissions to index** and click **Apply Changes**. You are brought back to the Source page.

9. When you are ready to start indexing the Twitter v2 source, click **Start**.

10. Validate that the source building process is executed without errors:

    • In the navigation panel on the left, click **Status**, and then validate that indexing proceeds without errors.

    OR
Open the CES Console to monitor source building activities.

What's Next?

- Set an incremental refresh schedule for your source.
- Consider modifying some hidden source parameters to try resolving other issues (see "Modifying Hidden Twitter v2 Source Parameters" on page 12).

9.42.6.1 Modifying Hidden Twitter v2 Source Parameters

The Add Source and Source: ... General pages of the Administration Tool present the parameters with which you can configure the Twitter v2 connector for most setups. More advanced, or seldom used parameters, are hidden. You can choose to make one or more of these parameters appear in the Add Source and Source: ... General pages of the Administration Tool so that you can change their default value. Consider changing hidden parameter values when you encounter issues, or when you want to fine tune connector performance.

The following list describes the advanced hidden parameters available with Twitter v2 sources. The parameter type (integer, string, etc.) appears between parentheses following the parameter name.

- **NumberOfRetries (Integer)**
  - The maximum number of times a failing request will be retried. The default value is 5.

- **RequestTimeout (Integer)**
  - The maximum amount of time (in seconds) an HTTP request can be executed before being canceled. The default value is 60.

- **RetrieveProtectedUsers (true, false)**
  - Whether or not to retrieve protected users. If this parameter is set to true, protected users and their Tweets will be accessible to everyone. The default value is false.

- **FollowedUsersPerPage (Integer)**
  - The number of users per page when retrieving users followed by a user, between 1 and 200. The default value is 200.

- **NumberOfUsersPerPage (Integer)**
  - The number of users per page when retrieving users from a list, between 1 and 5000. The default value is 5000.

- **TweetsPerTimelinePage (Integer)**
  - The number of Tweets per page when retrieving user timelines, between 1 and 200. The default value is 200.

- **TweetsPerSearchPage (Integer)**
  - The number of Tweets per page when retrieving Tweets from a search query, between 1 and 100. The default value is 100.

- **TweetsPerCollectionPage (Integer)**
  - The number of Tweets per page when retrieving Tweets from a collection, between 1 and 200. The default value is 200.
SearchResultsType (recent, mixed, popular)

The type of results retrieved with a search query, including mention Tweets. Can be either recent, mixed or popular. The default value is mixed.

Note: Popular usually returns around 15 Tweets.

SearchResultIsoLanguageCode

The ISO 639-1 language code to filter Tweets retrieved with a search query, including mention Tweets (does not work when retrieving Tweets from a user). The default value is none.

To modify hidden Twitter v2 source parameters

1. Refer to "Adding an Explicit Connector Parameter" on page 450 to add one or more Twitter v2 source parameters.

2. To modify parameter values, from the Administration Tool:

   - For a new Twitter v2 source:
     a. Select Index > Sources and Collections.
     b. Under Collections, select the collection in which you want to add the source.
     c. Under Sources, click Add.
     d. In the Add Source page, edit the newly added advanced parameter value.

   - For an existing Twitter v2 source:
     a. Select Index > Sources and Collections.
     b. Under Collections, select the collection containing the source you want to modify.
     c. Under Sources, click the existing Twitter source in which you want to modify the newly added advanced parameter.
     d. In the Source: ... General page, edit the newly added advanced parameter value.

3. Rebuild your Twitter v2 source to apply the changes to the parameters.

9.43 Web Pages Connector

The Web Pages connector allows to index web pages from one or more URLs. For websites with secured content, the connector supports source level file permissions as well as forms authentication.

Deployment overview

1. When the web pages that you want to index are on a secured web server, create a user identity that will contain the crawling account credentials (see "Adding a User Identity" on page 420).

Note: The Web Pages connector supports Kerberos authentication by impersonating a user defined in a user identity (with the user name in the username@domain form). The user must be from the same domain as the crawled web server.
2. Using the Coveo Administration Tool, configure and index a web source (see "Configuring and Indexing a Web Pages Source" on page 14).

3. For web sites with secured content:
   a. You can configure source level file permissions (see "Modifying Source Security Permissions" on page 297).
   b. When the website contains pages accessible only by filling forms, you can configure forms authentication (see "Indexing Secure Web Pages Using Forms" on page 300).

9.43.1 Configuring and Indexing a Web Pages Source

A source defines a set of connector parameters specifying where and how to crawl a website.

To configure and index a Web Pages source

1. On the Coveo server, access the Administration Tool.

2. Select Index > Sources and Collections.

3. In the Collections section:
   a. Select an existing collection in which you want to add the new source.
   OR
   b. Click Add to create a new collection.

4. In the Sources section, click Add.
   
   The Add Source page that appears is organized in three sections.

5. In the General Settings section of the Add Source page:
a. Enter the appropriate value for the following required parameters:

**Name**

Enter a descriptive name of your choice for the connector source.

*Example: My Organization Website*

**Source Type**

The connector used by this source. In this case, select **Web Pages**.

**Addresses**

The root URL for the website content that you want to index.

*Example: http://www.myorganization.com/*

You can also specify multiple URLs when they share the same configuration. This is useful when you want to index only specific sections of a website. Each URL must be on a separate line in the box.

*Note: It is recommended to create independent sources for independent websites.*

**Refresh Schedule**

Time interval at which the index is automatically refreshed to keep the index content up-to-date. By default, the **Every day** option instructs CES to refresh the source everyday at 12 AM. Choose the refresh rate appropriate to the rate at which the website content is updated.
Important: For a Web Pages source, the full refresh does not immediately catch deleted pages, but will remove a page from the index if the page returns a 404 error three times in a row. Otherwise, a rebuild eliminates deleted web pages from the index.

Note: You can create new or modify existing source refresh schedules.

b. Review the value for the following parameters that often do not need to be modified:

Rating

Change this value only when you want to globally change the rating associated with all items in this source relative to the rating to other sources.

Document Types

If you have defined custom document type sets, select the most appropriate one for this source.

Active Languages

If you have defined a custom language set for this source, select it.

Fields

If you have defined custom field sets, select the most appropriate one for this source.

6. In the Specific Connector Parameters & Options section of the Add Source page, review if you need to change the parameter default values:

User Agent

Determines the name used by the Web Pages connector to identify itself when downloading pages. Leave empty to use the default value (CoveoEnterpriseSearch) configured for all Web Pages sources in the Web Connector page (Configuration > Connectors > Web Crawler).

User Agent Identifier

Determines the identifier used by the Web Pages connector to identify itself when downloading pages.
Some websites use the user agent string ID to detect if the visitor is a specific browser or search engine crawler. The HTTP user agent id string field allows websites to check and detect browser and versions. This information can be used to output different HTML and content.

**Example:** Mozilla/5.0 (Windows; U; Windows NT 6.0; en-US) AppleWebKit/532.5 (KHTML, like Gecko) Safari/532.5

Leave empty to use the default value (Mozilla/4.0 (compatible; MSIE 5.0; Windows 95)) configured for all Web Pages sources in the Web Connector page (Configuration > Connectors > Web Crawler).

**Kerberos Cross Domain**

Specifies a semicolon separated list of Service Principal Names for cross domain authentication with Kerberos.

In the **Option** section:

**Index the document's metadata**

When selected, CES indexes all the document metadata, even metadata that are not associated with a field. The orphan metadata are added to the body of the document so that they can be searched.

When cleared (default), only the values of system and custom fields that have the **Free Text Queries** attribute selected will be searchable without using a field query.

**Example:** A document has two metadata:

- LastEditedBy containing the value Hector Smith
- Department containing the value RH

In CES, the custom field **CorpDepartment** is bound to the metadata **Department** and its **Free Text Queries** attribute is selected.

When the **Index the document's metadata** option is cleared, searching for RH returns the document because a field is indexing this value. Searching for hector does not return the document because no field is indexing this value.

When the **Index the document's metadata** option is selected, searching for hector also returns the document because CES indexed orphan metadata.

**Document's addresses are case-sensitive**

Select only when the addresses of website documents are case-sensitive. This option is cleared by default.

**Generate a cached HTML version of indexed documents**

Leave this check box selected (recommended). When indexing, CES creates HTML versions of indexed documents. In the search interfaces, users can then more rapidly review the content by clicking the Quick View link rather than opening the original web page. Consider clearing this check box only when you do not want to use Quick View links or save resources when building the source. This option is selected by default.
Open results with cached version

Leave this check box cleared (recommended) so that in the search interfaces, the main search result link opens the original web page. Consider selecting this check box only when you do not want users to be able to open the original web page but only see the HTML version of the document as a Quick View. In this case, you must also select Generate a cached HTML version of indexed documents. This option is cleared by default.

Reuse HTTP Connection

When crawling a website secured with Kerberos authentication, select this check box to keep the Kerberos connection alive between HTTP GET requests. This prevents repeating the Kerberos authentication for each request and can significantly improve the crawling performance.

Skip addresses with parameters (domain.com?parameters)

Select this check box to prevent CES from indexing pages whose addresses contain a query part that can return similar content, and therefore prevent indexing page duplicates and save disk space. Clear this check box when same addresses with different parameters return different content. This option is selected by default.

7. In the Security section of the Add Source page, when authentication is needed to crawl the website, enter the appropriate value for the following parameters:

![Security](image)

a. In the Authentication section, select one of the following options:

- **Crawl anonymously**
  
  Select when the full content of the website is available to everybody.

- **Crawl using the service identity**
  
  Select when the website is secured and the user identity of the CES service has full access to the website.

- **Crawl using this identity**
  
  Select when the website is secured and you want to use a specific user identity to crawl the website content (see "Adding a User Identity" on page 420).
**Note:** You can set up a Kerberos authentication to impersonate a user by creating and selecting a user identity for that user. The crawler threads will be impersonated with that user. The user must be from the same domain as the crawled web server. Consider selecting the Reuse HTTP Connection option.

b. In the **Security Provider** drop-down list, when you select to not crawl anonymously, select the security provider that can authenticate the user identity specified in the **Authentication** section.

c. Click **Save** to save the source configuration and start indexing this source.

8. When the website you are indexing uses Kerberos authentication and you assigned a Kerberos user identity to the source:

   ![Coveo Platform 7.0 | Administrator Guide](image)

   a. In the navigation panel on the left, select **Advanced**.

   b. **CES 7.0.6424+ (February 2014)** On the right, in the **Crawling** section, select the **Enable Kerberos authentication** option. NTLM or Basic authentication is used when the option is cleared.
Note: Consider clearing the **Enable Kerberos authentication** option to prevent getting error messages similar to the following:

An error occurred while warming up search page [URL]: class CGLNetwork::NetworkAccessDenied: The login information of server (SERVER NAME) is invalid.

9. Click **Start** to build your source.

10. Validate that the source building process is executed without errors:

   - In the navigation panel on the left, click **Status**, and then validate that the indexing proceeds without errors.

   OR

   - Open the CES Console to monitor the source building activities.

**What's Next?**

Source-level permissions are not indexed for Web Pages sources. However, when web page files are stored on the same network as the Coveo Master server, you can associate file server permissions to them (see "Modifying Source Security Permissions" on page 297).

CES also supports form-based authentication to access certain secure web pages (see "Indexing Secure Web Pages Using Forms" on page 300).

### 9.44 Yammer Connector

#### CES 7.0.6339+ (January 2014)

The Coveo connector for Yammer allows Coveo administrators to index and integrate Yammer network content into the Coveo unified index. The connector indexes all items from specified Yammer Basic and Yammer Enterprise network(s) so that in the Coveo search interfaces, a user can easily find this content.

**Note:** CES 7.0.8225+ (March 2016) The connector supports Yammer Enterprise.

#### 9.44.1 Features

The Yammer connector features are:

**Content indexing**

- Network
- Users
- Messages

  **Note:** Only group messages are indexed. Private conversation messages are ignored.

- Attachments (on messages)
Incremental refresh CES 7.0.8225+ (March 2016)

The connector periodically queries Yammer for the latest items modifications (addition, edition, deletion), keeping the index content up-to-date.

Feature History

<table>
<thead>
<tr>
<th>CES version</th>
<th>Monthly release</th>
<th>Features</th>
</tr>
</thead>
<tbody>
<tr>
<td>7.0.8225</td>
<td>March 2016</td>
<td>Add support for Yammer Enterprise</td>
</tr>
<tr>
<td>7.0.6339</td>
<td>January 2014</td>
<td>Connector prototype introduction</td>
</tr>
</tbody>
</table>

What's Next?

Review the steps to deploy the Yammer connector (see "Yammer Connector Deployment Overview" on page 21).

9.44.2 Yammer Connector Deployment Overview

The following procedure outlines the steps needed to deploy the Yammer connector. The steps indicate the order in which you must perform configuration tasks on both the Yammer and Coveo servers.

To deploy the Yammer connector

1. Validate that your environment meets the requirements (see "Yammer Connector Requirements" on page 22).
2. On the Yammer server:
   a. CES 7.0.8225+ (March 2016) (For Yammer Enterprise only) Enable private content mode:
      i. Log in to Yammer with a verified administrator account.
         
         **Note:** If your Yammer network is associated with Office 365, global admins in Office 365 are also verified admins in Yammer.

      ii. At the bottom of the navigation bar on the left, click the gear icon (Settings) and then click **Network Admin**.

      iii. Under **Content and security**, click **Content Mode**.

      iv. In the **Content Mode** page, select the **Private Content Mode** check box.

         **Important:** Selecting this option gives access to user private messages. However, private messages (not posted in a group) are NOT indexed by the connector.

      v. Click **Save**.

   b. (For a Yammer free network) Since there is no administrators, you must add a user in every groups from which you want to retrieve content using his account.

   c. Authorize the Coveo connector to access the content of your Yammer network:
i. Generate an access token (see Test Token).

ii. Take note of the access token that you will later need when configuring the user identity (see User identity).

3. On the Coveo server, in the Coveo Administration Tool:
   
a. Configure the user identity

   The connector needs an access token to authenticate to your Yammer network.

   **Notes:**
   - The User parameter is not used but cannot be left empty.
   - In the Password box, enter the access token that you just obtained (see Access Token).

   b. Optionally create an Email security provider

   When an email is defined for each of your users in Yammer and this email is used to authenticate them in your Coveo search interface, you can create an Email security provider to allow you to map your Yammer users to their email (see "Configuring an Email Security Provider" on page 65).

c. Configure a Yammer security provider

   A Yammer source needs a Yammer security provider (see "Configuring a Yammer Security Provider" on page 24).

d. Configure and index a Yammer source.

   The connector must know details about the Yammer network to index their content (see "Configuring and Indexing a Yammer Source" on page 26).

9.44.3 Yammer Connector Requirements

Your environment must meet the following requirements to be able to use the Coveo connector for Yammer:

- **CES 7.0.6339+ (January 2014)**

   The connector was introduced with the CES 7.0.6339 January 2014 release.

- Coveo license for the Yammer connector

   Your Coveo license must include support for the Yammer connector to be able to use this connector.

- Supported Yammer versions

   The connector supports Yammer Basic and Yammer Enterprise (CES 7.0.8225+ (March 2016)).

9.44.4 Authorizing the Coveo Connector to Access Your Yammer Network

You must perform the OAuth 2.0 protocol to authorize the Coveo connector to access the content of your Yammer network.
The OAuth 2.0 protocol is a protocol used for granting access to external applications without exposing the user’s real credentials. For the connector to be able to connect to the content of your network, it must acquire an access token.

To authorize the Coveo connector to access your Yammer network

1. Log into your Yammer network with a verified administrator account.

2. Create a registered application:
   a. Access the Registered applications page.
   b. In the Registered applications page, click Register New App.
   c. In the Register New App dialog that appears:

   ![Register New App dialog]

   All fields are required.

   - **Application Name**: Coveo Connector
   - **Organization**: MyCompany
   - **Support e-mail**: user@domain.com
   - **Website**: http://www.mycompany.com
   - **Redirect URI**: https://www.yammer.com

   By checking this box, you agree that you have read and agree to the Yammer API Terms of Service.
i. In the Application Name, Organization, Support e-mail and Website boxes, enter the values of your choice.


iii. Select the check box if you accept the terms and agreements.

iv. Click Continue.

d. In the [Application_Name] page, take note of the Client ID and Client Secret.

e. Open an internet browser.

f. Copy and paste the following URL in the browser address bar after entering your client ID and redirect URI at the specified places:


g. In the Connect[Application_Name] to your Yammer account page, click Allow.

h. In your browser address bar, take note of the authorization code returned by the Yammer API:

   https://www.yammer.com/[network]/?code=[authorization_code]#/home?code=[authorization_code]

i. Copy and paste the following URL in the browser address bar after entering your client ID, client secret and authorization code at the specified places:


j. Take note of the value next to token: in the resulting JSON as you will need the token when configuring the user identity (see Yammer Connector Deployment Overview).

What's Next?

Create a user identity (see Yammer Connector Deployment Overview).

9.44.5 Configuring a Yammer Security Provider

When you choose to index document permissions associated with Yammer items, the Coveo connector needs a security provider. When document permissions are indexed, in Coveo search results, a user searching for Yammer content only sees the content to which he has access in Yammer.

Note: You can get familiar with how Coveo components deal with permissions on documents both at indexing and query time.

To configure a Yammer security provider

1. On the Coveo server, access the Administration Tool.


3. In the navigation panel on the left, click Security Providers.
4. In the **Security Providers** page, click **Add** to create a new security provider.

5. In the **Modify Security Provider** page:

![Modify Security Provider page](image)

   a. Configure the following required parameters:

   **Name**
   
   Choose a significant name to identify the security provider.

   **Example:** Yammer Security Provider

   **Security Provider Type**
   
   Select **Yammer (x64)**.

   **User Identity**
   
   Select the Yammer user identity that you created previously.

   **Security Provider**
   
   Select an email security provider that you created to allow this Yammer security provider to map Yammer users (permissions) to email users.

   b. Review the following parameter value that often does not need to be changed:
User cache refresh time in seconds

The maximum interval in seconds after which the user cache is reset. The default value is 3,600 seconds (1 hour).

c. Leave the Allow Complex Identities option cleared as it does not apply to this type of security provider.
d. Click Apply Changes.

What's Next?

Configure and index a Yammer source (see "Configuring and Indexing a Yammer Source" on page 26).

9.44.6 Configuring and Indexing a Yammer Source

A source defines a set of configuration parameters for a specific Yammer network.

To configure and index a Yammer source

1. On the Coveo server, access the Administration Tool.
2. Select Index > Sources and Collections.
3. In the Collections section:
   a. Select an existing collection in which you want to add the new source.
   OR
   b. Click Add to create a new collection.
4. In the Sources section, click Add.
   The Add Source page that appears is organized into three sections.
5. In the General Settings section of the Add Source page:
a. Enter the appropriate value for the following required parameters:

**Name**

A descriptive name of your choice for the connector source.

**Example:** Yammer Enterprise

**Source Type**

The connector used by this source. In this case, select **Yammer**.

**Note:** If you do not see **Yammer** in the Source Type list, ensure that your environment meets the requirements (see "Yammer Connector Requirements" on page 22).

**Addresses**

The URL of your Yammer network.

**Example:** https://www.yammer.com/[companyDomain]

b. The following parameters often do not need to be changed:

**Rating**

Change this value only when you want to globally change the rating associated with all items in this source relative to the rating of other sources.
Example: When the source indexes a legacy repository, you may want to set this parameter to **Low**, so that in the search interface, results from this source appear lower in the list compared to those from active repository sources.

**Document Types**

If you defined a custom document type set for this source, select it.

**Active Languages**

If you defined custom active language sets, ensure to select the most appropriate for this source.

**Fields**

If you created a custom Yammer field set for this source, select it. Otherwise, leave the **Default Scheme**.

**Refresh Schedule**

Time interval at which the index is automatically refreshed to keep the index content up-to-date. By default, the **Every day** option instructs CES to refresh the source everyday at 12 AM. Because the incremental refresh takes care of maintaining the source up-to-date, you can select a longer interval such as **Every Sunday**.

6. In the **Specific Connector Parameters & Options** section of the **Add Source** page:

   a. In the **Mapping File** box, optionally enter the path to a mapping file that should apply to the items in this source.

   Leave this box empty to use the default mappings that should be appropriate in most cases.

   **CES 7.0.8225+ (March 2016)** When the default mappings do not fulfill your needs, you can use the Coveo.CES.CustomCrawlers.Yammer.MappingFile.xml file (located in the Coveo Enterprise Search 7 Bin folder) as a starting point or contact Coveo Support for assistance. Your XML mapping file must respect the standard Coveo mapping file schema.

   b. The **Option** check boxes generally do not need to be changed:

   **Index Subfolders**

   Keep this check box selected (recommended). By doing so, all subfolders from the specified server
address are indexed.

Index the document's metadata

When selected, CES indexes all the document metadata, even metadata that are not associated with a field. The orphan metadata are added to the body of the document so that they can be searched using free text queries.

When cleared (default), only the values of system and custom fields that have the Free Text Queries attribute selected will be searchable without using a field query.

Example: A document has two metadata:
- LastEditedBy containing the value Hector Smith
- Department containing the value RH

In CES, the custom field CorpDepartment is bound to the metadata Department and its Free Text Queries attribute is selected.

When the Index the document's metadata option is cleared, searching for RH returns the document because a field is indexing this value. Searching for hector does not return the document because no field is indexing this value.

When the Index the document's metadata option is selected, searching for hector also returns the document because CES indexed orphan metadata.

Document's addresses are case-sensitive

Leave the check box cleared. This parameter needs to be checked only in rare cases for systems in which distinct documents may have the same name but different casing.

Generate a cached HTML version of indexed documents

When you select this check box (recommended), at indexing time, CES creates HTML versions of indexed documents. In the search interfaces, users can then more rapidly review the content by clicking the Quick View link rather than opening the original document with the original application. Consider clearing this check box only when you do not want to use Quick View links or to save resources when building the source.

Open results with cached version

Leave this check box cleared (recommended) so that in the search interfaces, the main search result link opens the original document with the original application. Consider selecting this check box only when you do not want users to be able to open the original document but only see the HTML version of the document as a Quick View. In this case, you must also select Generate a cached HTML version of indexed documents.

7. In the Security section of the Add Source page:
a. In the **Authentication** drop-down list, select the Yammer crawling user identity that you created for this source (see *Yammer Connector Deployment Overview*).

b. In the **Security Provider** drop-down list, select the Yammer security provider that you created for this source (see "Configuring a Yammer Security Provider" on page 24).

c. Click **Save and Start** to save the source configuration and build the source.

8. Validate that the source building process is executed without errors:

   - In the navigation panel on the left, click **Status**, and then validate that the indexing proceeds without errors.

   OR

   - Open the CES Console to monitor the source building activities.

### 9.45 YouTube Connector

**CES 7.0.7433+ (February 2015)**

The Coveo connector for YouTube allows Coveo administrators to index and integrate YouTube user and brand channels content into the Coveo unified index. The connector indexes all items from specified YouTube channel(s) so that in the Coveo search interfaces, a user can easily find this content.

#### 9.45.1 Connector Features Summary

<table>
<thead>
<tr>
<th>Features</th>
<th>Supported</th>
<th>Additional information</th>
</tr>
</thead>
<tbody>
<tr>
<td>YouTube version</td>
<td>Data API (v3)</td>
<td></td>
</tr>
<tr>
<td>Searchable content types</td>
<td>✔️</td>
<td>Metadata on videos, channel playlists, and playlist items.</td>
</tr>
</tbody>
</table>
9.45.2 Features

The YouTube connector features are:

Content indexing

- Extraction and indexing of all available YouTube metadata on videos (including thumbnails).
- CES 7.0.7711+ (June 2015) YouTube channel playlists and playlist items are indexed, but channel related playlists, such as the Likes and Watch Later, are not indexed.

Partial Incremental refresh

YouTube channels are periodically re-indexed by the connector to catch newly uploaded videos (see "Configuring and Indexing a YouTube Source" on page 36).

Notes:

- Private and unpublished videos are not indexed.
- Deleted and changed videos require a full refresh to be taken in account (see Limitation).

Pause/Resume

When indexing YouTube content, the connector can be paused and resumed.

9.45.3 Limitation

- Limited incremental refresh capabilities:
  - A full refresh is needed to update deleted videos
  - A full refresh is needed to update changes on videos
  - A full refresh is needed to update statistics on videos (e.g., view counts, likes, ...)

Permissions must be manually defined on the source [more]
A full refresh is needed to update playlists and playlist items.

Note: CES 7.0.7711+ (June 2015) Playlist and Playlist items of a YouTube channel are indexed.

What's Next?

Review the steps to deploy the YouTube connector (see "YouTube Connector Deployment Overview" on page 32).

9.45.4 YouTube Connector Deployment Overview

The following procedure outlines the steps needed to deploy the YouTube connector. The steps indicate the order in which you must perform configuration tasks on both the Google and Coveo servers.

To deploy the YouTube connector

1. Validate that your environment meets the requirements (see "YouTube Connector Requirements" on page 32).

2. On the Google server, create a Google API Console project to allow the Coveo connector access to the YouTube channel(s) of your choice (see "Allowing the Coveo Connector Access to YouTube Data" on page 33).

3. On the Coveo server, in the Coveo Administration Tool:

   a. Create a YouTube field set to take advantage of the available YouTube metadata.
      i. It is recommended to start by importing the default YouTube field set file ([CES_Path]Bin\Coveo.CES.CustomCrawlers.YouTube.FieldSet.xml) to create fields for all the metadata available by default from YouTube videos.
      ii. When you created custom metadata for your YouTube documents, add corresponding fields to the field set.

   b. Configure and index a YouTube source.

      The connector must know details about the YouTube channels to index their content (see "Configuring and Indexing a YouTube Source" on page 36).

   c. If you encounter issues, verify if modifying the default value of hidden source parameters can help resolve the problems (see "Modifying Hidden YouTube Source Parameters" on page 42).

9.45.5 YouTube Connector Requirements

Your environment must meet the following requirements to be able to use the YouTube connector:

- CES 7.0.7433+ (February 2015)

- Coveo license for the YouTube connector

Your Coveo license must include support for the YouTube connector to be able to use this connector.

- A valid Google Account

Using a Google Account, you must log in the Google API Console to authorize Coveo access to YouTube data (see Allowing the Coveo Connector Access to YouTube Data).
What's Next?

The YouTube connector needs an API (YouTube Data API v3) to identify itself to Google. The connector uses this API, which is a link between the connector and the YouTube channels, to access the public videos that you want to index (see “Allowing the Coveo Connector Access to YouTube Data” on page 33).

9.45.6 Allowing the Coveo Connector Access to YouTube Data

The Coveo connector uses a Google API (YouTube Data API v3) to retrieve information about the different items in YouTube (videos, users, channels). You must enable the YouTube Data API v3 API and create an API key to authorize the Coveo connector to access the YouTube public content that you want to index.

**Note:** The YouTube Data API v3 API does not provide account information or give any sort of authentication rights.

To allow the connector access to YouTube data

1. Go to the Google Developers Console, and log in using a Google Account.

2. Create a service account project for the Coveo connector:

   **Note:** You can also select an existing project and start this step from substep c.

   a. In the Projects page, click Create Project.

   b. In the New Project dialog box, enter a project name and ID, and then click Create.
c. Click your [Project Name].

d. Access the APIs page:
   - In the sidebar on the left, click APIs & auth, and then click APIs.
   - OR
   - In the Project Dashboard page, click Enable an API.

e. In the APIs page, ensure that for YouTube Data API v3, the Status is set to ON.

3. In the sidebar on the left, under APIs & auth, select Credentials, and then in the Public API access section, click the Create new key button.
4. In the next **Create a new key** dialog box, click the **Server key** button.

5. In the **Create a server key and configure allowed IPs** dialog box that appears, click **Create**.

   **Note:** When you want to limit the utilization of your API key, you can enter your server path, meaning that only the requests from your server will be accepted.
Create a server key and configure allowed IPs

This key should be kept secret on your server.

Every API request is generated by software running on a machine that you control. Per-user limits will be enforced using the address found in each request’s userIp parameter, (if specified). If the userIp parameter is missing, your machine’s IP address will be used instead. Learn more

ACCEPT REQUESTS FROM THESE SERVER IP ADDRESSES

One IP address or subnet per line. Example: 192.168.0.1, 172.16.0.0/16, 2001:db8::1 or 2001:db8::64

Create  Cancel

6. Back in the Google Developers Console, in the Key for server applications section, take note of the API key that you will need later to configure your YouTube source.

9.45.7 Configuring and Indexing a YouTube Source

A source defines a set of configuration parameters for a specific YouTube channel.

To configure and index a YouTube source

1. On the Coveo server, access the Administration Tool.
2. Select Index > Sources and Collections.
3. In the **Collections** section:
   
   Select an existing collection in which you want to add the new source.
   
   OR
   
   Click **Add** to create a new collection.

4. In the **Sources** section, click **Add**.

   The **Add Source** page that appears is organized in three sections.

5. In the **General Settings** section of the **Add Source** page:

   ![Add Source page](image)

   a. Enter the appropriate value for the following required parameters:

   **Name**
   
   Enter a descriptive name of your choice for the connector source.
   
   **Example:** The Company YouTube Channel

   **Source Type**
   
   Select the connector used by this source. In this case, select **YouTube**.
   
   **Note:** If you do not see **YouTube**, your environment does not meet the requirements (see "YouTube Connector Requirements" on page 32).
Addresses

Enter the URL of one or more YouTube user or brand channels, or playlists.

Example:

- https://youtube.com/channel/channelID
- https://youtube.com/user/username
- https://youtube.com/playlist?list=playlistID

Notes:

- When you enter a URL pointing to a specific user who manages more than one channels, the connector indexes all videos under these channels.

  * CES 7.0.8541+ (September 2016) The connector supports playlist URLs.

Fields

Select the field set that you created for your YouTube source (see YouTube Connector Deployment Overview).

Refresh Schedule

Time interval at which the index is automatically refreshed to keep the index content up-to-date. By default, the Every day option instructs CES to refresh the source everyday at 12 AM. Because the incremental refresh takes care of maintaining the source up-to-date, you can select a longer interval such as Every Sunday.

b. Review the value for the following parameters that often do not need to be modified:

Rating

Change this value only when you want to globally change the rating associated with all items in this source relative to the rating to other sources.

Example: When a source replaces a legacy system, you may want to set this parameter to High, so that in the search interface, results from this source appear earlier in the list compared to those from legacy system sources.

Document Types

If you defined a custom document type set for this source, select it.

Active Languages

If you defined custom active language sets, ensure to select the most appropriate for this source.

6. In the Specific Connector Parameters & Options section of the Add Source page:
a. In the **API Key** box, enter the API key you previously created (see *Allowing the Coveo Connector Access to YouTube Data*).

b. In the **Mapping File** box, the path to the default mapping file that defines how the connector handles metadata often does not need to be changed.

c. **CES 7.0.8388+ (June 2016)** Select the **Index Playlists** check box when you want YouTube channel playlists and playlist items to be indexed.

Notes:

- **CES 7.0.8541+ (September 2016)** This option is not used when you specify a playlist URL in the User, Channel, or Playlist URL parameter.
- **CES 7.0.8225– (March 2016)** YouTube channel playlists and playlist items are indexed by default.

d. Click **Add Parameter** when you want to show and change the value of advanced source parameters (see "Modifying Hidden YouTube Source Parameters" on page 42).

e. The **Option** check boxes generally do not need to be changed:

**Index Subfolders** **CES 7.0.7599– (April 2015)**  
This parameter is not taken into account for this connector.

**Index the document’s metadata**

When selected, CES indexes all the document metadata, even metadata that are not associated with a field. The orphan metadata are added to the body of the document so that they can be searched using free text queries.

When cleared (default), only the values of system and custom fields that have the **Free Text Queries** attribute selected will be searchable without using a field query.
Example: A document has two metadata:
- LastEditedBy containing the value Hector Smith
- Department containing the value RH

In CES, the custom field CorpDepartment is bound to the metadata Department and its Free Text Queries attribute is selected.

When the **Index the document's metadata** option is cleared, searching for RH returns the document because a field is indexing this value. Searching for hector does not return the document because no field is indexing this value.

When the **Index the document's metadata** option is selected, searching for hector also returns the document because CES indexed orphan metadata.

Document's addresses are case-sensitive **CES 7.0.7433–(February 2015)**

Ensure that this option is selected since YouTube video IDs are case sensitive.

**Generate a cached HTML version of indexed documents**

When you select this check box (recommended), at indexing time, CES creates HTML versions of indexed documents. In the search interfaces, users can then more rapidly review the content by clicking the **Quick View** link rather than opening the original document with the original application. Consider clearing this check box only when you do not want to use **Quick View** links or to save resources when building the source.

**Open results with cached version**

Leave this check box cleared (recommended) so that in the search interfaces, the main search result link opens the original document with the original application. Consider selecting this check box only when you do not want users to be able to open the original document but only see the HTML version of the document as a **Quick View**. In this case, you must also select **Generate a cached HTML version of indexed documents**.

f. Click **Save** to save the source configuration.

7. Since the YouTube connector only indexes public videos, security permissions on the source content must be disabled:
a. In the navigation menu on the left, select **Permissions**.

b. Next to **Permissions**, select the **Specifies the security permissions to index** option.

c. Next to **Allowed Users**, ensure that a well-known everyone group such as the Active Directory `everyone \S-1-1-0\` is added.

d. Click **Apply Changes**.

e. On the toolbar, click **Rebuild** to start indexing your source.

8. Validate that the source building process is executed without errors:

   - In the navigation panel on the left, click **Status**, and then validate that the indexing proceeds without errors.

   OR

   - Open the CES Console to monitor the source building activities.

What's Next?

Set an incremental refresh schedule for your source.
Consider modifying some hidden source parameters to try resolving other issues (see "Modifying Hidden YouTube Source Parameters" on page 42).

9.45.7.1 Modifying Hidden YouTube Source Parameters

The **Add Source** and **Source: ... General** pages of the Administration Tool present the parameters with which you can configure the connector for most YouTube setups. More advanced and more rarely used parameters are hidden. You can choose to make one or more of these parameters appear in the **Add Source** and **Source: ... General** pages of the Administration Tool so that you can change their default value. Consider changing values of hidden parameters when you encounter issues.

The following list describes the advanced hidden parameters available with YouTube sources. The parameter type (integer, string, etc.) appears between parentheses following the parameter name.

**IndexPlaylistItems (Boolean) CES 7.0.8541+ (September 2016)**

Whether playlist items are indexed. The default value is true. When set to false, playlist item titles are only displayed in the ytplaylistitemstitle field.

**BatchSize (Integer)**

Number of items to fetch per request made to the YouTube server. The default value is 30 items. The minimum value is 1 item. A small value forces the connector to make small but frequent queries to YouTube. A larger value leads to larger and less frequent queries.

**LastRefreshCushion (Integer)**

The time set in minutes to ensure the incremental refresh catches all newly uploaded videos. The default value is 180 minutes.

**Note:** Since the Google API (YouTube Data API v3) has a latency, add this parameter to set the incremental refresh to look for newly uploaded videos during a wider time interval. Without this parameter, if an incremental refresh runs before an uploaded video is available to be caught (YouTube must finish processing the video), the video would not be indexed.

To modify hidden YouTube source parameters

1. Refer to "Adding an Explicit Connector Parameter" on page 450 to add one or more YouTube source parameters.

2. For a new YouTube source, access the **Add Source** page of the Administration Tool to modify the value of the newly added advanced parameter:
   a. Select **Index > Sources and Collections**.
   b. Under **Collections**, select the collection in which you want to add the source.
   c. Under **Sources**, click **Add**.
   d. In the **Add Source** page, edit the newly added advanced parameter value.

3. For an existing YouTube source, access the **Source: ... General** page of the Administration Tool to modify the...
value of the newly added advanced parameter:

a. Select **Index > Sources and Collections**.

b. Under **Collections**, select the collection containing the source you want to modify.

c. Under **Sources**, click the existing YouTube source in which you want to modify the newly added advanced parameter.

d. In the **Source: ... General** page, edit the newly added advanced parameter value.

4. Rebuild your YouTube source to apply the changes to the parameters.

### 9.46 Zendesk Connector

**CES 7.0.7914+ (October 2015)**

The Coveo connector for Zendesk allows Coveo administrators to index and integrate the content of a Zendesk customer service website into the Coveo unified index. The connector indexes all items from a Zendesk customer service website so that in the Coveo search interfaces, a user can easily find Zendesk content.

#### 9.46.1 Features

The Zendesk connector features are:

**Content indexing**

Extraction and indexing of the following Zendesk item types:

- Tickets
- Users
- Groups
- Organizations
- Articles
- Comments
- Attachments

**Note:** Since the part of the Zendesk API v2 for the Help Center is in beta, the content of Help Center communities (topics, questions, ideas and posts) cannot yet be indexed.

**Mostly supported security model CES 7.0.8047+ (December 2015)**

The connector depends on a part (User Segments) of the Zendesk API v2 to retrieve permissions for indexed items. Since the part of the API for the Help Center is in beta, the permissions can currently only be indexed for tickets and their sub-items (comments and attachments). This means that, in Coveo search interfaces, a user searching Zendesk content only sees the tickets to which they have access in Zendesk.
Notes:

- The Zendesk API v2 does not provide the permissions for the following item types: articles and their sub-items (comments and attachments). Most of the time, the Help Center content is public, meaning that the articles are made available to all end-users and agents, but in some cases, you may have restricted the access to some sections and categories (see [Restricting access to knowledge base content]).

- CES 7.0.9272+ (March 2018) The Access Policies API has been removed by Zendesk on December 15, 2017 and replaced by User Segments (see [Sunsetting] Access Policies for Help Center).

Incremental refresh CES 7.0.8047+ (December 2015)

Supports incremental refresh to periodically query Zendesk for the latest edits, keeping the index content up-to-date.

Multithreading

The connector can run multiple threads, which can improve performances considerably (see Modifying Hidden Zendesk Source Parameters).

Partial Pause/Resume CES 7.0.8047+ (December 2015)

When indexing Zendesk ordered items such as tickets and articles, the connector can be paused and resumed.

9.46.2 Limitations

- CES 7.0.7914 (October 2015) The connector does not yet support Zendesk permissions.

Important: In the Coveo search interface, a user searching Zendesk content could see content to which he has normally no access in Zendesk. Thus, it is currently highly recommended to only index Zendesk customer service websites with public content.

Since Zendesk APIs can only be used by Zendesk admin users, it is currently impossible to limit the content to be indexed to a certain organization, group, or user (agent and end-user).

- CES 7.0.7914 (October 2015) A full refresh is needed to retrieve the latest items modifications (addition, edition, deletion).

What's Next?

Review the steps to deploy the Zendesk connector (see "Zendesk Connector Deployment Overview" on page 44).

9.46.3 Zendesk Connector Deployment Overview

The following procedure outlines the steps needed to deploy the Zendesk connector. The steps indicate the order in which you must perform configuration tasks on both the Zendesk and Coveo servers.

To deploy the Zendesk connector

1. Validate that your environment meets the requirements (see "Zendesk Connector Requirements" on page 46).

2. (When you want the connector to connect to your Zendesk content using OAuth 2.0 - recommended method)
   - On the Zendesk server, create an application to authorize the Coveo connector to access your Zendesk content

www.coveo.com
3. On the Coveo server, in the Coveo Administration Tool:
   a.  **CES 7.0.8047+ (December 2015)** Optionally create security providers

   When you want to index Zendesk permissions, you must create two security providers to get Zendesk item permissions and resolve and expand groups. Due to a Zendesk API v2 limitation, not all permissions are currently retrievable (see Permission limitation).

   In Zendesk, users are identified by their email addresses. Consequently, permissions returned by the Zendesk security provider for each document are email addresses. The Zendesk security provider then requires another security provider to uniquely identify users from their email addresses.

   i. Start by selecting or creating a security provider that the Zendesk security provider will use to resolve and expand groups. The security provider type to use depends on how users are authenticated when they access the search interface:

      **Note:** You may require to also use a REGEX Transform Member Name security provider in between the two following security providers to map member member types. Contact Coveo Support for assistance.

      - When authenticated with their email address, use an Email security provider (see "Configuring an Email Security Provider" on page 65).

      - When authenticated with an Active Directory account, use an LDAP Lookup security provider that maps LDAP identities to Active Directory ones. Contact Coveo Support for assistance.

      **Note:** This chain of security providers is required since the Zendesk security provider does not directly support to be chained with an Active Directory security provider.

   ii. Then, create a Zendesk security provider that the connector uses to resolve indexed permissions (see "Configuring a Zendesk Security Provider" on page 49).

   b. (When you want the connector to connect to your Zendesk content using a Zendesk API v2 token) Configure a user identity.

   The connector needs to know the username of a Zendesk admin account by creating a CES user identity that you will later associate to your Zendesk source.

      **Note:** This method is not recommended since the Zendesk API token allows read and write permissions.

   c. Create a Zendesk field set to take advantage of the available Zendesk metadata.

      i. It is recommended to start by importing the default Zendesk field set file \([CES_Path]\Bin\Coveo.CES.CustomCrawlers.Zendesk.FieldSet.xml\) to create fields for all the metadata available by default from Zendesk documents.

      ii. When you created custom metadata for your Zendesk documents, add corresponding fields to the field set.

   d. Configure and index a Zendesk source.
The connector must know details to access and index the Zendesk content of your managed users (see "Configuring and Indexing a Zendesk Source" on page 52).

e. If you encounter issues, verify if modifying the default value of hidden source parameters can help resolve the problems (see "Modifying Hidden Zendesk Source Parameters" on page 57).

9.46.4 Zendesk Connector Requirements

Your environment must meet the following requirements to be able to use the Zendesk connector:

- **CES 7.0.7914+ (October 2015)**
- Coveo license for the Zendesk connector
  
  Your Coveo license must include support for the Zendesk connector to be able to use this connector.
- A valid admin Zendesk account
  
  Using an administrator Zendesk account, you must create a Zendesk app and an OAuth 2.0 protocol to authorize Coveo to access the content of your Zendesk customer service website (see Authorizing the Coveo Connector to Access Your Zendesk Content).

What's Next?

Grant Coveo access to the content of your Zendesk customer service website by creating a Zendesk application (see "Authorizing the Coveo Connector to Access Your Zendesk Content" on page 46).

9.46.5 Authorizing the Coveo Connector to Access Your Zendesk Content

You can grant the Coveo connector access to your Zendesk customer service website content using a Zendesk API v2 token. It is however recommended to perform the complete OAuth 2.0 protocol for security reasons (can grant the access to your Zendesk content with only read permission).

The OAuth 2.0 protocol is a protocol used for granting access to external applications without exposing the user’s real credentials. For the connector to be able to connect to the content of your Zendesk customer service website, it must acquire an access token.

To authorize the Coveo connector to access your Zendesk content

1. Log into your Zendesk customer service website with an administrator account.
2. Access the agent interface, by clicking the drop-down list menu in the top right of the page, and then selecting **Open agent interface**.
3. In the agent interface, access the **Zendesk API** page:
   a. In the navigation bar on the left, click the Admin icon.
   b. In the admin setting menu, under **Channels**, click **API**.
4. In the **Zendesk API** page, depending on the way you want to grant access to your Zendesk content:
Using OAuth 2.0

a. Click the OAuth Clients tab.

b. In the OAuth Clients tab, click add a client.

c. In the New OAuth Client page:
   
   i. In the Client Name box, enter a descriptive application name.

   Example: Coveo Connector

   ii. Take note of the Unique Identifier auto-populated. You need this value during the OAuth authentication process.

   iii. In the Redirect URLs box, enter http://localhost/.

   iv. Click Save.

   v. Take note of your application Secret.

   vi. Click Save again.

d. Authorize your application to use your Zendesk administrator account:

   i. Open another browser tab by pressing CTRL+t.

   ii. In the new tab, copy and paste the following URL in the browser address bar after entering your website and client ID at the specified places: https://[YOUR WEBSITE].zendesk.com/oauth/authorizations/new?response_type=token&redirect_url=http://localhost/&client_id=[YOUR_UNIQUE_IDENTIFIER]&scope=read.

   iii. In the Allow [ClientName] to access your Zendesk account screen, click Allow to receive an authorization code from Zendesk.
You are redirected to the URI you specified when configuring the Zendesk app.

iv. In your browser address bar, take note of the access token returned by the Zendesk API. You need this value when configuring your Zendesk source (see Configuring and Indexing a Zendesk Source).

Example: http://localhost/#access_token={ACCESS_TOKEN}&scope=read&token_type=bearer

- Using a Zendesk API v2 token:
  a. In the Zendesk API page, in the Settings tab, next to Token Access, select the Enabled check box.
  b. In the section that appears, click add new token.
  c. In the Enter a label for this API Token dialog that appears, enter a descriptive name, and then click Create.

Example: CoveoConnector

d. Back in the API page, next to Token Access, select the Enabled check box.

e. Under Active API tokens, take note of the API token. You need this value when configuring your Zendesk source (see Configuring and Indexing a Zendesk Source).

f. Click Save.
What's Next?

Create a Zendesk source ("Configuring and Indexing a Zendesk Source" on page 52).

9.46.6 Configuring a Zendesk Security Provider

The Coveo Zendesk connector mostly supports the Zendesk security model. Due to a Zendesk API v2 limitation, not all permissions are currently retrievable (see Permission limitation). When you want users searching for Zendesk tickets and their sub-items (comments and attachments) in a Coveo search interface to only see the tickets to which they have access in Zendesk, the connector needs a security provider to be able to index the permissions for each indexed ticket.

Note: You can get familiar with how Coveo components deal with permissions on documents both at indexing and query time.

To configure a Zendesk security provider

1. On the Coveo server, access the Administration Tool.
3. In the navigation panel on the left, click Security Providers.
4. In the Security Providers page, click Add to create a new security provider.
5. In the Modify Security Provider page:
a. Configure the following required parameters:

**Name**

Choose a meaningful name to identify the security provider.

*Example:* Zendesk Security Provider

**Security Provider Type**

In the drop-down list, select **Zendesk (x64)**.

**User Identity**

Depending on the method you chose to retrieve your Zendesk content, in the drop-down list (see "Authorizing the Coveo Connector to Access Your Zendesk Content" on page 46):

- Using an OAuth 2.0 access token (recommended method), select *(none)*.
- Using a Zendesk API v2 token, select the user identity you previously created (see Zendesk Connector Deployment Overview).
b. Configure the following required parameters with the same values as the ones you will enter when configuring the source (see "Configuring and Indexing a Zendesk Source" on page 52):

**API Token**

(When you want the connector to retrieve your Zendesk content using a Zendesk API v2 token) Enter the API token previously obtained (see Authorizing the Coveo Connector to Access Your Zendesk Content).

*Note:* This method is not recommended since the Zendesk API token allows read and write permissions.

*Example:* FAwrsE3RdyBxqkVDHJeYvqJYr70TM1DzyUNIBpql

**Access Token**

(When granting the connector access to your Zendesk content using OAuth 2.0) Enter the access token previously obtained (see Authorizing the Coveo Connector to Access Your Zendesk Content).

*Example:* fdbefa0cb05bc3641481496d44af60b05cf3rrj3406t299b6cc5789608d4d9f83

**Zendesk Server URL**

Enter the base URL of your Zendesk customer service website.

*Example:* https://company.zendesk.com

**CES 7.0.9272+ (March 2018) Only index permissions for agents and administrators**

Select this checkbox to only retrieve Agent and Administrator entity permissions. End users permissions are not indexed when this option is selected.

**CES 7.0.9272+ (March 2018) Index permissions from specific organizations only**

Enter the Zendesk organizations of which you want to index the permissions. Use a semi-colon to separate your values.

*Example:* MyOrganization1;MyOrganization2

**Cache Expiration CES 7.0.9167+ (December 2017)**

Enter the absolute expiration (in minutes) for a cache entry. By default, a cache entry expires after 60 minutes.

**Security Provider**

Select the security provider that you selected or created to allow this security provider to resolve and expand the groups (see Zendesk Connector Deployment Overview).

c. Select the security provider that you selected or created to allow this security provider to resolve and expand the groups (see Zendesk Connector Deployment Overview).

d. Leave the **Allow Complex Identities** checkbox cleared as it does not apply to this type of security provider.

e. Click **Apply Changes**.
What's Next?

Create and index a source (see "Configuring and Indexing a Zendesk Source" on page 52).

9.46.7 Configuring and Indexing a Zendesk Source

A source defines a set of configuration parameters for a specific Zendesk customer service website.

To configure and index a Zendesk source

1. On the Coveo server, access the Administration Tool.

2. Select Index > Sources and Collections.

3. In the Collections section:
   a. Select an existing collection in which you want to add the new source.
   OR
   b. Click Add to create a new collection.

4. In the Sources section, click Add.

   The Add Source page that appears is organized in three sections.

5. In the General Settings section of the Add Source page:
a. Enter the appropriate value for the following required parameters:

**Name**

Enter a descriptive name of your choice for the connector source.

*Example: Zendesk*

**Source Type**

Select the connector used by this source. In this case, select *Zendesk*.

*Note: If you do not see Zendesk, your environment does not meet the requirements (see "Zendesk Connector Requirements" on page 46).*

**Addresses**

Enter the base URL of your Zendesk customer service website.

*Example: https://company.zendesk.com*

**Fields**

Select the field set that you created earlier (see Zendesk Connector Deployment Overview).

**Refresh Schedule**

Time interval at which the index is automatically refreshed to keep the index content up-to-date. By default, the *Every day* option instructs CES to refresh the source everyday at 12 AM. Because the incremental refresh takes care of maintaining the source up-to-date, you can select a longer interval such as *Every Sunday*.

*Note: CES 7.0.7914 (October 2015) Keep the *Every day* option as the incremental refresh is not supported.*

b. Review the value for the following parameters that often do not need to be modified:

**Rating**

Change this value only when you want to globally change the rating associated with all items in this source relative to the rating to other sources.

*Example: When a source replaces a legacy system, you may want to set this parameter to High, so that in the search interface, results from this source appear earlier in the list compared to those from legacy system sources.*

**Document Types**

If you defined a custom document type set for this source, select it.

**Active Languages**

If you defined custom active language sets, ensure to select the most appropriate for this source.

6. In the *Specific Connector Parameters & Options* section of the *Add Source* page:
a. Using the following parameters, authorize the Coveo crawler to access the content of your Zendesk customer service website:

**API Token** Security provider

(When you want the connector to retrieve your Zendesk content using a Zendesk API v2 token) Enter the API token to use that you previously obtained (see Authorizing the Coveo Connector to Access Your Zendesk Content).

Note: This method is not recommended since the Zendesk API token allows read and write permissions.

**Access Token** Security provider

(When granting the connector access to your Zendesk content using OAuth 2.0) Enter the access token to use that you previously obtained (see Authorizing the Coveo Connector to Access Your Zendesk Content).

b. In the **Mapping File** box, the path to the default mapping file that defines how the connector handles metadata often does not need to be changed.

c. The following options must be selected for certain Zendesk item types to be indexed.

**Index Comments**

Whether the comments on tickets and articles should be indexed.

**Index Administration Entities CES 7.0.8047+ (December 2015)**

Whether the users, groups and organizations should be indexed. By default, administration entities are not indexed.
Index Tickets CES 7.0.8996+ (June 2017)

Whether tickets should be indexed.

Index Help Center Articles CES 7.0.8996+ (June 2017)

Whether the articles in the Help Center should be indexed.

Index Help Center Items CES 7.0.8047 to CES 7.0.8850 (December 2015 to March 2017)

Whether the articles and their attachments should be indexed. By default, Help Center items are indexed.

d. (Optional) Click Add Parameter when you want to show and change the value of advanced source parameters (see "Modifying Hidden Zendesk Source Parameters" on page 57).

e. The Option check boxes generally do not need to be changed:

Index Subfolders

This parameter is not taken into account for this connector.

Index the document's metadata

When selected, CES indexes all the document metadata, even metadata that are not associated with a field. The orphan metadata are added to the body of the document so that they can be searched using free text queries.

When cleared (default), only the values of system and custom fields that have the Free Text Queries attribute selected will be searchable without using a field query.

**Example:** A document has two metadata:

- LastEditedBy containing the value Hector Smith
- Department containing the value RH

In CES, the custom field CorpDepartment is bound to the metadata Department and its Free Text Queries attribute is selected.

When the Index the document's metadata option is cleared, searching for RH returns the document because a field is indexing this value. Searching for hector does not return the document because no field is indexing this value.

When the Index the document's metadata option is selected, searching for hector also returns the document because CES indexed orphan metadata.

Document's addresses are case-sensitive

Leave the check box cleared. This parameter needs to be checked only in rare cases for systems in which distinct documents may have the same name but different casing.

Generate a cached HTML version of indexed documents

When you select this check box (recommended), at indexing time, CES creates HTML versions of indexed documents. In the search interfaces, users can then more rapidly review the content by...
clicking the **Quick View** link rather than opening the original document with the original application. Consider clearing this check box only when you do not want to use **Quick View** links or to save resources when building the source.

**Open results with cached version**

Leave this check box cleared (recommended) so that in the search interfaces, the main search result link opens the original document with the original application. Consider selecting this check box only when you do not want users to be able to open the original document but only see the HTML version of the document as a **Quick View**. In this case, you must also select **Generate a cached HTML version of indexed documents**.

7. In the **Security** section of the **Add Source** page:

![Security settings](image)

**Important:** **CES 7.0.7914 (October 2015)** The connector does not yet support Zendesk permissions. It is thus strongly recommended to only index Zendesk customer service websites with public content.

**Note:** A workaround is to manually define permissions on the source (see Permissions).

a. In the **Authentication** drop-down list, depending on your setup:

- When you grant the connector access to your content using OAuth, select **(none)**.
- When you grant the connector access to your content using the Zendesk API, select the user identity you previously created (see Zendesk Connector Deployment Overview).

b. **CES 7.0.8047+ (December 2015)** When you chose to index Zendesk permissions, in the **Security Provider** drop-down list, select the Zendesk security provider that you created for this source (see “Configuring a Zendesk Security Provider” on page 49 and Permission limitation).

8. Click **Save** to save the source configuration.

9. When your Zendesk content is all public:
Important: CES 7.0.7914 (October 2015) The connector does not yet support Zendesk permissions. This means that, in the Coveo search interface, a user searching Zendesk content could see content to which he has normally no access in Zendesk.

Since Zendesk APIs can only be used by Zendesk admin users, it is currently impossible to limit the content to be indexed to a certain organization, group, or user (agent and end-user).

Note: When your Zendesk content is not public, a workaround is to enter the name of user(s) or group(s) you want to allow or deny access to your organization content in the Allowed Users and Deny Users boxes.

a. In the navigation panel on the left, click Permissions.

b. In the Permissions page, select Specify the security permissions to index.

c. In the Allowed Users and Denied Users boxes, enter the users and groups that you respectively want to allow or deny to see search results from this source. The default is to allow everyone \S-1-1-0\ (Active Directory Group).

d. Click Apply Changes.

10. When you are ready to start indexing the Zendesk source, click Rebuild.

11. Validate that the source building process is executed without errors:

   - In the navigation panel on the left, click Status, and then validate that the indexing proceeds without errors.
   
   OR

   - Open the CES Console to monitor the source building activities.

What’s Next?

Set an incremental refresh schedule for your source.

Consider modifying some hidden source parameters to try resolving other issues (see “Modifying Hidden Zendesk Source Parameters” on page 57).

9.46.7.1 Modifying Hidden Zendesk Source Parameters

The Add Source and Source: ... General pages of the Administration Tool present the parameters with which you can configure the connector for most Zendesk setups. More advanced and more rarely used parameters are hidden. You can choose to make one or more of these parameters appear in the Add Source and Source: ... General pages of the Administration Tool so that you can change their default value. Consider changing values of hidden parameters when you encounter issues.

The following list describes the advanced hidden parameters available with Zendesk sources. The parameter type (integer, string, etc.) appears between parentheses following the parameter name.

NumberOfRefreshThreads (Integer)

The number of refresh threads used by the crawler for this source. The default value is 4.
To modify hidden Zendesk source parameters

1. Refer to "Adding an Explicit Connector Parameter" on page 450 to add one or more Zendesk source parameters.

2. For a new Zendesk source, access the Add Source page of the Administration Tool to modify the value of the newly added advanced parameter:
   a. Select Index > Sources and Collections.
   b. Under Collections, select the collection in which you want to add the source.
   c. Under Sources, click Add.
   d. In the Add Source page, edit the newly added advanced parameter value.

3. For an existing Zendesk source, access the Source: ... General page of the Administration Tool to modify the value of the newly added advanced parameter:
   a. Select Index > Sources and Collections.
   b. Under Collections, select the collection containing the source you want to modify.
   c. Under Sources, click the existing Zendesk source in which you want to modify the newly added advanced parameter.
   d. In the Source: ... General page, edit the newly added advanced parameter value.

4. Rebuild your Zendesk source to apply the changes to the parameters.

9.47 Shared Connector Topics

This section contains topics that are applicable to more than one connector.

9.47.1 Standard Mapping File Schema

A Coveo connector may need a mapping file to correctly copy the repository metadata values to appropriate index fields. This topic describes the format of the standard mapping file by providing its XML schema definition. Refer to this schema to review the possible content of the file and ensure that your mapping file is valid.
Notes:

- **CES 7.0.7914+ (October 2015)** Using a mapping file, in a field or body element, you can retrieve the content of an external file by setting the `isUrl` attribute to `true` in the start tag and entering the external file URL as the value.

  **Example:**

  ```xml
  <Field name="contact" isUrl="true">%[UrlMetadata]/</field>
  ```

  The normal mapping resolution is performed and when the download attempt of the resolved value is successful, the downloaded content is converted to a string and put in the body or field element. One use case is when you have a database with a column containing a URI that points to a document that you want to use as a body.

  When using this feature, have in mind that:

  - `isUrl` is case-sensitive.
  - Direct mapping (ex: `<Field name="[value]" isUrl="true">[value]/</Field>`) and mapping resolution (ex: `<Body isUrl="true">%[File_Path_or_URL]/</Body>`) are both supported schemes.
  - Old mappings are compatible, meaning that when `isUrl` is not specified, the attribute is considered set to `false` (no download is performed).
  - The specified external file can be a `.PDF`, `.DOCS`, `.ETC`, `.TXT`, `.RTF` or `.HTML` file and its URL can start with `http://`, `https://` or `file://`.
  - The content of the external file must be public since no authentication is supported when performing the download attempt.
  - When an invalid URL is specified, an error message stating that a mapping fails is logged, but the document is still indexed.

- By default, when the name of a field in the field set selected for the source matches the name of a metadata from the indexed repository, the metadata value is automatically copied to the field, even when they are not formally associated in a mapping file.

- The standard mapping file schema is supported by all connectors written in C# (all connectors except Web Legacy). However, it is recommended for the connectors that use their own mappings (such as Oracle UCM) to NOT mix these specific mappings with standard ones.

- Some connectors come with a default mapping file that is available in the `[CES_Path]\bin` folder. The mapping file name is in the form:

  Coveo.CES.CustomCrawlers.[ConnectorName].MappingFile.xml

  When a default mapping file is available, it is recommended to start with its content by using and customizing a copy of the file.

This mapping file format is used by more recently developed or updated connectors. This standard mapping file only contains metadata to field mappings, not other connector configuration parameters. When needed, a connector rather uses a separate configuration file for non-mapping parameters.

The format of the mapping file version 1 is specified in the following XML schema definition (XSD).
<?xml version="1.0" encoding="utf-8"?>
<xs:schema xmlns:xs="http://www.w3.org/2001/XMLSchema">

<!-- definition of possible elements -->
<xs:element name="Mappings">
  <xs:complexType>
    <xs:sequence>
      <xs:element name="Version" minOccurs="1" maxOccurs="1"/>
      <xs:element name="CommonMapping" minOccurs="0" maxOccurs="1" type="GenericMapping"/>
      <xs:element name="Mapping" minOccurs="0" maxOccurs="unbounded" type="SpecificMapping"/>
      <xs:element name="DefaultMapping" minOccurs="0" maxOccurs="1" type="GenericMapping"/>
    </xs:sequence>
  </xs:complexType>
</xs:element>

<!-- definition of generic (common and default) mapping section -->
<xs:complexType name="GenericMapping">
  <xs:group ref="MappingElement"/>
</xs:complexType>

<!-- definition of a specific mapping section -->
<xs:complexType name="SpecificMapping">
  <xs:group ref="MappingElement"/>
  <xs:attribute name="type" use="required"/>
</xs:complexType>

<!-- definition of a mapping element -->
<xs:group name="MappingElement">
  <xs:element name="Title" minOccurs="0" maxOccurs="1"/>
  <xs:element name="Body" minOccurs="0" maxOccurs="1"/>
  <xs:element name="ClickableUri" minOccurs="0" maxOccurs="1"/>
  <xs:element name="PrintableUri" minOccurs="0" maxOccurs="1"/>
  <xs:element ref="Fields" minOccurs="0" maxOccurs="1"/>
</xs:group>

<!-- definition of fields element -->
<xs:element name="Fields">
  <xs:complexType>
    <xs:sequence>
      <xs:element ref="Field" minOccurs="0" maxOccurs="unbounded"/>
    </xs:sequence>
  </xs:complexType>
</xs:element>

<!-- definition of field element -->
<xs:element name="Field">
  <xs:complexType>
    <xs:simpleContent>
      <xs:extension base="xs:string">
        <xs:attribute name="name" use="required"/>
      </xs:extension>
    </xs:simpleContent>
  </xs:complexType>
</xs:element>
</xs:schema>
Example: The JIVE connector uses the standard mapping file schema:

```xml
<?xml version="1.0" encoding="utf-8" ?>
<Mappings>
  <Version></Version>
  <CommonMapping>
    <Fields>
      <Field name="sysauthor">%{author.displayName}</Field>
      <!-- Jive system fields -->
      <Field name="syscstag">%{tags}</Field>
      <Field name="syscstaggroup">%{categories}</Field>
      <Field name="syscsplace">%{coveo.places.titles}</Field>
      <Field name="syscsplacetype">%{coveo.places.types}</Field>
    </Fields>
  </CommonMapping>
  <Mapping type="announcement">
    <Title>%{subject}</Title>
    <Body><![CDATA[<html>%{content.text}</html>]]></Body>
    <Fields>
      <Field name="sysfiletype">csannouncement</Field>
      <!-- Jive system fields -->
      <Field name="syscsitemtype">Announcement</Field>
    </Fields>
  </Mapping>
  <Mapping type="attachment">
    <Title>%{name}</Title>
    <Fields>
      <Field name="sysfilename">%{name}</Field>
    </Fields>
  </Mapping>
  <Mapping type="checkpoint">
    <Title>%{name}</Title>
    <Body>%{description}</Body>
    <Fields>
      <Field name="sysdtdue">dueDate</Field>
      <Field name="sysfiletype">cscheckpoint</Field>
      <!-- Jive system fields -->
      <Field name="syscsitemtype">Checkpoint</Field>
    </Fields>
  </Mapping>
  <Mapping type="comment">
    <Title>%{subject}</Title>
    <Body><![CDATA[<html>%{content.text}</html>]]></Body>
    <Fields>
      <Field name="sysfiletype">cscomment</Field>
      <!-- Jive system fields -->
      <Field name="syscsitemtype">Comment</Field>
    </Fields>
  </Mapping>
  <Mapping type="discussion">
    <Title>%{subject}</Title>
    <Body><![CDATA[<html>%{content.text}</html>]]></Body>
    <Fields>
      <Field name="sysfiletype">csdiscussion</Field>
      <!-- Jive system fields -->
      <Field name="syscsitemtype">Discussion</Field>
    </Fields>
  </Mapping>
  <Mapping type="dm">
    <Title>%{subject}</Title>
    <Body><![CDATA[<html>%{content.text}</html>]]></Body>
    <Fields>
      <Field name="sysfiletype">csdm</Field>
      <!-- Jive system fields -->
      <Field name="syscsitemtype">dm</Field>
    </Fields>
  </Mapping>
</Mappings>
```
<Field name="syscsitemtype">Poll</Field>
</Mapping>

<Mapping type="post">
<Title>%[subject]</Title>
<Body><![CDATA[ <html> %[content.text] </html> ]]]></Body>
<Fields>
<Field name="sysfiletype">csblogpost</Field>
<!-- Jive system fields -->
<Field name="syscsitemtype">Blog Post</Field>
</Fields>
</Mapping>

<Mapping type="project">
<Title>%[name]</Title>
<Body>%[description]</Body>
<Fields>
<Field name="sysdtdue">dueDate</Field>
<Field name="sysauthor">%[creator.displayName]</Field>
<Field name="sysfiletype">csproject</Field>
<!-- Jive system fields -->
<Field name="syscsitemtype">Project</Field>
</Fields>
</Mapping>

<Mapping type="space">
<Title>%[name]</Title>
<Body>%[description]</Body>
<Fields>
<Field name="sysfiletype">cscommunity</Field>
<!-- Jive system fields -->
<Field name="syscsitemtype">Community</Field>
</Fields>
</Mapping>

<Mapping type="systemblog">
<Title>%[name]</Title>
<Body>%[description]</Body>
<Fields>
<Field name="sysfiletype">cssystemblog</Field>
<!-- Jive system fields -->
<Field name="syscsitemtype">System Blog</Field>
</Fields>
</Mapping>

<Mapping type="task">
<Title>%[subject]</Title>
<Body><![CDATA[ <html> %[content.text] </html> ]]]></Body>
<Fields>
<Field name="sysdtdue">dueDate</Field>
<Field name="sysfiletype">cstask</Field>
<!-- Jive system fields -->
<Field name="syscstaskassignedto">%[owner.extra.displayName]</Field>
</Fields>
</Mapping>

<Mapping type="update">
<Title>%[subject]</Title>
<Body><![CDATA[ <html> %[content.text] </html> ]]]></Body>
<Fields>
<Field name="sysfiletype">csupdate</Field>
<!-- Jive system fields -->
<Field name="syscsitemtype">Update</Field>
</Fields>
</Mapping>

<Mapping type="video">
<Title>%[subject]</Title>
<Body><![CDATA[ <html> %[content.text] </html> ]]]></Body>
<Fields>
<Field name="sysfiletype">csvideo</Field>
<!-- Jive system fields -->
<Field name="syscsitemtype">Video</Field>
</Fields>
</Mapping>
9.47.2 Finding Available Metadata

You may find that it is often not simple to identify the metadata available in indexed documents. This topic explains how to use the AllFieldValues postconversion script to help you extract and review all the available metadata in the documents of a repository.

To find available metadata

1. Make the AllFieldValues postconversion script available to CES:
   
   a. Save the content of the following script in the **[Index_Path]\Scripts\Postconversion-allfieldvalues.txt** text file on the Coveo Master server:

   ```vbs
   Option Explicit
   ' This postconversion script sample adds a new metadata named
   ' "AllFieldValues". This new metadata contains the name, the value and the
   ' type of all document metadata.
   '******************************************************************************
   Dim DOUBLE_QUOTE: DOUBLE_QUOTE = chr(34)
   Dim allValues: allValues = "<AllFieldValues>" & vbNewLine
   Dim fieldNames: fieldNames = DocumentInfo.Fields
   ' For each document field name.
   Dim fieldName
   For Each fieldName In fieldNames
      ' Get the field value.
      Dim fieldValue: fieldValue = DocumentInfo.GetFieldValue(CStr(fieldName))
      ' Add the metadata name and its value to the buffer variable.
      allValues = allValues & "<Field"
      allValues = allValues & " name=" & DOUBLE_QUOTE & CStr(fieldName) & DOUBLE_QUOTE
      allValues = allValues & " value=" & DOUBLE_QUOTE & fieldValue & DOUBLE_QUOTE
      allValues = allValues & " type=" & DOUBLE_QUOTE & TypeName(fieldValue) & DOUBLE_QUOTE
      allValues = allValues & " />" & vbNewLine
   Next
   allValues = allValues & "</AllFieldValues>" & vbNewLine
   '******************************************************************************

   Call DocumentInfo.SetFieldValue("AllFieldValues", allValues & "</AllFieldValues>" & vbNewLine)
   ```

   b. Add the postconversion script in the Administration Tool using the following values (see "Adding a Postconversion Script" on page 462):
   
   - **Name**: AllFieldValues
   - **Script File**: **[Index_Path]\Scripts\Postconversion-allfieldvalues.txt**
   - **Script Language**: VBScript

2. Associate the AllFieldValues postconversion script with the source for which you want to see all available
metadata (see "Applying a Source Conversion Script" on page 465).

3. Add the AllFieldValues custom field to the field set used by the source:
   a. If needed, create a new field set to be used by this source (see "Adding a Field Set" on page 491).
   b. Add the AllFieldValues custom field to the appropriate field set using the following values (see "Adding or Modifying Custom Fields" on page 494).
      - Name: AllFieldValues
      - Type: String
      - Metadata Name: AllFieldValues
   c. Ensure that the source uses the field set that contains the AllFieldValues custom field (see "Modifying the Field Set Used by a Source" on page 498).

4. If not already done, rebuild the source to populate the AllFieldValues field for all documents of the source.

5. Use the Index Browser to review the available metadata (see "Reviewing Document Details from the Index Browser" on page 375).

What's Next?

Create custom fields with the useful metadata listed in the AllFieldValues field. Use the Field name value as your metadata name (see "Adding or Modifying Custom Fields" on page 494).

9.47.3 Configuring an Email Security Provider

An Email security provider is a simple email user identity container that can be used by another security provider to recognize users by their email addresses. When used by more than one security providers attached to sources of various types, an email security provider can act as a single sign-on system. An Email security provider does not connect to any system so it does not need a user identity.

Note: You can get familiar with how Coveo components deal with permissions on documents both at indexing and query time.

To configure an Email security provider

1. On the Coveo server, access the Administration Tool.
3. In the navigation panel on the left, select Security Providers.
5. In the Modify Security Provider page:
a. In the **Name** box, enter a name of your choice for your Email security provider.

b. In the **Security Provider Type** list, select **Email**.

**Note:** CES 7.0.5785 to 7.0.5935 (August to September 2013) The Email security provider DLL file is missing in the CES distribution so you will not see the **Email** option in the **Security Provider Type** list.

To resolve this issue:

i. Contact Coveo Support to get a copy of the Coveo.CES.CustomCrawlers.EmailSecurityProvider.dll file.

ii. When you receive the file, using an administrator account, connect to the Coveo Master server, and then copy the file to the \[CES_Path]\bin folder.

iii. When your Coveo instance includes a Mirror server, also copy the file to the \[CES_Path]\bin folder on the Coveo Mirror server.

iv. Restart the CES service so that the new DLL is recognized.

c. In the **User Identity** list, leave **(none)**.

d. CES 7.0.7814+ (August 2015) (Optional) In the **Security Provider** list, select another security provider to map Email identities to another identity type.
Example: You want to map Email identities to Active Directory (AD) ones so you select an LDAP Lookup security provider that is chained to an AD security provider. The LDAP Lookup security provider is then able to find a user in AD from his email and extracts his User Principal Name (UPN), thus allowing a mapping of the Email identity to an AD one. Contact Coveo Support for assistance on how to create an LDAP Lookup security provider.

e. Leave the Allow Complex Identities option cleared as it does not apply to this type of security provider.

f. Click Apply Changes.

What's Next?

Configure a security provider that will use this Email security provider.

9.47.4 Configuring a REGEX Transformation Security Provider

The Coveo Member Name Regex Transformation security provider, is a special type of security provider that uses matching and replacement regular expressions (REGEX) to only transform member names received from one security provider type to another name format for another security provider type. A REGEX Transformation security provider is always configured in sandwich between two other security providers.

Some kind of rule must allow to transform the member name from its input format to the output format using regular expressions. You must be proficient with regular expressions to configure this type of security provider.

Example: You have a Google Drive source in which account names are user emails (username@mycompany.com), but your users are authenticated with their Active Directory (AD) account (mycompany\username) when they access a Coveo search interface. For users to be granted to see Google Drive documents in search results, document permissions must be associated to their AD account, otherwise, no results will be returned.

As shown in the following diagram, you can accomplish this by configuring your Google Drive source to get permissions from a Google Drive security provider that sends output members to the REGEX Transformation security provider, which finally outputs transformed member names to the Active Directory security provider, so that at the end, the permissions of the Google Drive account are available in the security cache for the equivalent AD account.

![Diagram showing the configuration process](image)

Note: You can get familiar with how Coveo components deal with permissions on documents both at indexing and query time.

To configure a REGEX Transformation security provider

1. On the Coveo server, access the Administration Tool.

3. In the Security page, in the navigation panel on the left, click Security Providers.

4. In the Security Providers page, click Add to create a new security provider.

5. In the Modify Security Provider page:

   ![Security Provider Configuration](image)

   a. In the Name box, enter a name to identify this security provider.

   **Example**: If you configure the security provider to transform names from the email format to the AD format:

   Email to AD REGEX Transform

   b. In the Security Provider Type drop-down list, select Coveo Member Name Regex Transformation.

   c. In the User Identity drop-down list, leave the selection to (none), because this parameter is not applicable to this type of security provider.

   d. In the Security Provider section, select the output security provider to which transformed names will be sent.
Example: When this security provider output name format is AD, select the out-of-the-box Active Directory security provider.

e. In the Match regex (input) box, enter the regular expression to match and select appropriate parts of your input name format.

Example: To match parts of an email address:

```
([\w-\.]+)@[\w]+([a-zA-Z]{2,4})
```

f. In the Replace regex (output) box, enter the replacement regular expression for your output name format.

Example: To convert the email name to an Active Directory name for the mycompany domain:

```
mycompany\$1
```

Important: Fully test your matching and replacement regular expressions to ensure they transform member names as expected for all member name cases.

g. Select the Case sensitive users check box when the account names are case sensitive.

h. CES 7.0.8996+ (June 2017) Select the Only Map Matched Members check box if you wish to map only members whose name matches the regex specified by the Match Regex (Input) parameter.

i. In the Parameters section, in rare cases, Coveo Support could instruct you to click Add Parameters to specify other security provider parameter names and values that could help to resolve or troubleshoot security provider issues.

j. Leave the Allow Complex Identities option cleared as it does not apply to this type of security provider.

k. Click Apply Changes.

What's Next?

Assign this REGEX Transformation security provider as an output for the appropriate other security provider.
10. Coveo REST Search API 8.0

The Coveo Platform 7 comes with the Coveo Search API, a REST web service that is used by other Coveo products such as the Coveo JavaScript Search Framework to send queries and receive search results from a Coveo unified index. The Coveo Search API REST endpoint can also be used by custom applications (see REST Search API Home).

As shown in the following diagram, the Coveo Search API acts as a bridge between the front-end search interfaces or applications and a Coveo Enterprise Search (CES) instance maintaining a unified index on the back-end. The Coveo Search API is typically installed on the Coveo Master server, together with CES, but you can install it on any server (see "Installing the Coveo Search API" on page 92).

Once installed, you can configure various aspects of the Coveo Search API such as the index server, certificates, and authentication (see "Customizing and Starting the Coveo Search API" on page 95).

10.1 Creating a Search API Hosted JavaScript Search Page

Search API 8.0.457+ (March 2015)

The Coveo Search API comes bundled with the Coveo JavaScript Search framework and can conveniently host one or more search pages. Authorized users can create and modify search pages hosted by the Search API using the JavaScript Search Legacy Interface Editor.

To create a JavaScript Search Page to be hosted in by the Search API

1. Ensure that the Search API v8.0.457+ is installed on a server and configured to connect with a Coveo Enterprise Search server (see "Installing the Coveo Search API" on page 92, "Customizing and Starting the Coveo Search API" on page 95, and Identifying the REST Search API Version).

2. Configure the Search API searchPageDesigners permissions:

   You must configure who can create and modify search pages hosted by the Search API.

   a. Using an administrator account, connect to the server on which the Search API is installed.

   b. Using a text editor, open the search API configuration file [Search_API_Path]\config.yml (by default C:\Program Files\Coveo Search API 8\config.yml).

   c. In the file, ensure that the windowsAuthentication or basicAuthentication, as well as the admin...
sections are configured in the file:

- When users are authenticated as Active Directory users:

  Add a `windowsAuthentication` section in which the `provider` value matches the Coveo Enterprise Search (CES) security provider name (by default `Active Directory`).

  In the `admin` section:

    - The `provider` value must be `Windows` to indicate that users are authenticated using the `windowsAuthentication` method.
    - The `searchPageDesigners` section determines who can create and modify search pages hosted by the Search API.

  **Example:** In the following configuration, only `MYDOMAIN\username3` and members of the `Administrators` group can create and edit search pages.

    ```
    windowsAuthentication:
      enabled: true
      provider: Active Directory

    admin:
      enabled: true
      provider: Windows
      groups: 
        - name: Administrators
          members: ["MYDOMAIN\username1","MYDOMAIN\username2"]
      searchPageDesigners:
        - MYDOMAIN\username3
        - Administrators
    ```

  **Note:** For a Windows provider, you cannot specify Active Directory group names. You must rather specify individual users.

  OR

- When users are not authenticated:

  Add a `basicAuthentication` section to rather define users in the Search API configuration file. You must include a `provider` parameter with a CES security provider name as the value (such as `Active Directory`), but this security provider is not used for the purpose of the `admin` section.

  In the `admin` section:

    - The `provider` value must be `Basic` to indicate that users are authenticated using the `basicAuthentication` method.
    - The `users` section defines each user and the associated password BCrypt hash.

      You must choose the for each user, encrypt it using a BCrypt tool, copy the BCrypt hash in the section, and communicate the password to each user.
Note: You can find online BCrypt tools (such as the BCrypt Calculator) to encrypt and test encrypted hashes against passwords.

Example: In the following configuration, only members of the MyDesigners group (username2 and username3) can create and modify search pages hosted by the Search API.

```
basicAuthentication:
   enabled: true
   provider: Active Directory

admin:
   enabled: true
   provider: Basic

users:
   - name: username1
     hash: $2a$04$DqADemxWjVVbBsdWzR4/c0OTwPDXI3aXpDlGlLlU0F8ElakMFJmkPm
   - name: username2
     hash: $2a$04$kZsiWWieKKAHJA1K06OB4.reFSbYB3N9XEuGo9381y7gR/lM.I17W
   - name: username3
     hash: $2b$343feNiWVeKKAsKDu6d$fwbphYDS.6tIgj84n00fD9sdsf8924d3bJ

administrators:
   - username1

groups:
   - name: MyDesigners
     members: ["username2", "username3"]

searchPageDesigners:
   - MyDesigners
```

Important: The syntax in config.yml YAML file is picky:

- Respecting the indentation is critical. An indentation level must be two spaces, not a tabulation (the presence of one or more tab characters in the file will prevent the Search API service to start!). Some text editors may automatically insert tabs when adding lines. If possible configure your text editor to show all characters minimize risks of creating an invalid configuration file.

- When specifying Windows users:
  - The domain or machine name MUST BE in capital letters (ex.: MYCOMPANY\myusername).
  - When specifying a user in an array, the username must be within quotes and a backslash character (\) must be escaped with another backslash (ex.: ["MYDOMAIN\\username1","MYDOMAIN\\username2"]).
  - When specifying one user, you do not need quotes and must not escape backslash characters (ex.: MYDOMAIN\username3).

- The complete config.yml file specifications are available from the Coveo Developers site (see Windows Service Configuration File).

  d. Save the config.yml file.
  
  e. Restart the Coveo Search API service to make changes effective:
i. In the Windows Services window, right-click Coveo Search API, and then select Restart (see How to Access Services Window in Windows XP, Windows 7 & 8).

ii. Ensure that the Coveo Search API service does not immediately stop. If it is the case, your config.yml file is invalid. You must identify and fix syntax errors.

3. In a browser, to start the creation process for the default search page, enter the URL of the Search API server with the port and without a path name.

**Examples:**
- When the Coveo Search API is deployed on the machine which hostname is search, the URL using the default port (8080) would be:
  
  http://search.mycompany.com:8080

- When the browser currently runs on the server where the Coveo Search API is installed, you can use:
  
  http://localhost:8080

**Note:** You can change the port used by the Coveo Search API by setting the port attribute in the http section of the config.yml file (see The http Section).

OR

To create a search page with a custom name, enter the URL of the Search API server followed by the desired name in the path.

**Example:** When the Coveo Search API is deployed on the machine which hostname is search, the URL using the default port (8080) could be:

http://search.mycompany.com:8080/MyAwesomeSearchPage

which will create a MyAwesomeSearchPage.html file.

4. With a browser that does not support integrated authentication or when basic authentication is configured for searchPageDesigners permissions, in the browser log in dialog box that appears, enter your username and password.

If your credentials are not recognized, contact your Search API administrator to validate that you are authorized to create and modify search pages and which authentication method is used.

5. In the This Search Page Is not Configured Yet dialog box, click the Click Here to Start button to launch the search page creation process.
6. In the **Setup Search Page** dialog:

   a. You can disable one or more suggested tabs corresponding to the found index content.

   b. Optionally, click **More Tabs**, when you want to immediately add tabs for other types of sources that are not yet indexed.

   Note: Added tabs will contain no results until you index content of the corresponding type.

   You can always add or remove tabs later using the Legacy Interface Editor (see Making Basic JavaScript Search Page Customization With the Legacy Interface Editor).

   c. Click **Create Page**.

   The search page appears.

   The search page files are saved on the Search API server in the \[Search_API_Path]\pages\ folder (by default \C:\Program Files\Coveo Search API 8\pages\). The default search page file name is default.html.
What's Next?

Use the Legacy Interface Editor to customize the page (see "Accessing the JavaScript Search Legacy Interface Editor for a Search API Hosted Page" on page 75).

Note: The Legacy Interface Editor is also bundled with Coveo for Salesforce and its usage is documented in the Coveo for Salesforce online help (see JavaScript Search Legacy Interface Editor Overview).

10.2 Accessing the JavaScript Search Legacy Interface Editor for a Search API Hosted Page

Coveo Search API 8.0.457 (March 2015)

The Coveo Search API can host Coveo JavaScript Search pages (see "Creating a Search API Hosted JavaScript Search Page" on page 70). Once such a search page is available, authorized users can modify the page using the JavaScript Search Legacy Interface Editor.

To access the Legacy Interface Editor for a JavaScript Search page hosted in the Search API

1. Ensure that the installed Coveo Search API version is 8.0.457 (March 2015 monthly release) or later (see Identifying the REST Search API Version).

   If you have an older version, download the latest Search API 8 version and update your server to this version.

2. Using a browser, access a Search API hosted search page by entering the URL of the page.

   Examples:

   - When the Coveo Search API is deployed on a machine which hostname is search with the default port (8080), the URL to access the default search page URL could be:
     http://search.mycompany.com:8080
   - When the browser currently runs on the server where the Coveo Search API is installed, you can use:
     http://localhost:8080
   - To access a custom search page, simply add the page file name to the server URL:
     http://search.mycompany.com:8080/MyAwesomeSearchPage.html

3. In the Interface Editor lower-right corner, click the Interface Editor menu button ( ).

   Note: If you do not see the Interface Editor menu button ( ), or nothing happens when clicking it, you either do not have permissions to create or modify the search page or the installed Coveo Search API version is prior to version 8.0.457.

4. When not already authenticated, in the browser login dialog box that appears, enter your credentials.

5. In the Interface Editor menu, click Edit.
The Interface Editor appears in a side panel on the right.

What's Next?

Learn what you can do with the JavaScript Search Interface Editor (see Making Basic JavaScript Search Page Customization With the Interface Editor).
11. Third-Party System Procedures

Coveo Platform 7 works within the same operating system as other third-party software. Thus, some configuration in these software may be needed in order to setup Coveo Platform properly, such as modifications in the Microsoft Windows Registry Editor or the creation of a database in a Microsoft SQL server. This section regroups topics that are referred from other topics in the online help.

11.1 About the Microsoft .NET Framework

The Microsoft .NET Framework is an integral Windows component that enables building and running software applications. It also includes ASP.NET, a technology for Web applications.

The Coveo Platform user interfaces (search interfaces, Administration Tool, Interface Editor, and Console) use the Microsoft .NET Framework (see "Third-Party Software Requirement" on page 7). The framework must therefore be installed on the Coveo server. The Coveo installers verify if the proper version of the Microsoft .NET Framework is installed on the server and installs it when it is missing.

**Note:** The Coveo installers however require that at least the .NET Framework 2 be available to operate. When it is missing, for example on fresh Windows server installations, you must manually install the Microsoft .NET Framework 3.5 that includes the .NET Framework 2 (see the Microsoft page Microsoft .NET Framework 3.5), and then restart the installer.

11.2 Microsoft Registry Editor

This section regroups topics related to the Microsoft Windows Registry Editor, which is a tool used to view and change settings in the system registry. When installing a new program, such as Coveo Platform, Windows refers to and updates the information contained in the system registry. Thus, you may need to access the Microsoft Windows Registry Editor and change the value of some Coveo registry keys when the Coveo unified index path is modified (see "Changing the Coveo Index Path in the Registry Editor" on page 77).

11.2.1 Opening the Registry Editor

You may need to access the Microsoft Windows Registry Editor to change some Coveo configuration.

To open the Registry Editor

1. Using an administrator account, connect to the server on which you want to edit the registry.
2. On the Windows Start menu, select Run.
3. In the Run dialog box, in the Open box, type regedit.

The Registry Editor window appears.

11.2.2 Changing the Coveo Index Path in the Registry Editor

You may need to change the value of some Coveo registry keys when the index path is modified, for example when you relocate the Coveo unified index.
To change the Coveo index path in the Registry Editor

1. Open the Registry Editor (see "Opening the Registry Editor" on page 77).

2. In the Computer tree, expand the following sections: HKEY_LOCAL_MACHINE > SOFTWARE > Coveo > Enterprise Search > 7 > Instance > Default.

3. In the list of registry keys appearing in the panel on the right, for the ConfigPath and ConfigTempPath registry keys:
   a. Double-click the registry key.
   b. In the Edit String dialog box, enter the new path of the index folder.

   **Example:** When the new index folder is D:\CES7, enter D:\CES7\Config\.

   c. Click OK.

4. Close the Registry Editor window.

11.3 Microsoft IIS and the Coveo Platform

The Coveo Platform includes web-based user interfaces that require a web server to run their application (such as the Administration Tool, Interface Editor, and search interface). The Coveo web applications operate with Microsoft Internet Information Services (IIS), the web server available for all supported Microsoft Windows editions. The Coveo installers deploy IIS when it is missing and create the necessary Coveo web sites.

**Note:** Only the .exe version of the Coveo installers automatically installs IIS. The .msi version does not (see the Microsoft document [Methods of Installing IIS 7.0 and Above](#)).

11.3.1 Finding the Name of the User that Runs a Process in IIS

The Coveo administrator may need to know the identity of the user that runs a process in Microsoft Internet Information Services (IIS) to be able to set the permission for that user in another system.

To find the name of the user that runs a process in IIS 7

1. On the IIS server, start the IIS Manager (on the Windows taskbar, select Start > Administrative Tools > Internet Information Services (IIS) Manager).

2. In Internet Information Services (IIS) Manager:
   a. In the Connections panel, under Sites, select the site for which you want to know the user identity.

   **Example:** Select Coveo Enterprise Search 7.

   b. In the Actions panel on the right, click Basic Settings.

   c. In the Edit Site dialog box that appears, note the name of the Application pool, and then click OK.
Example: Classic .NET AppPool in the figure.

Example: NetworkService in the figure.

d. In the Connections panel, select Application Pools, and then note the name in the Identity column for the applicable Application Pool.

11.3.2 Finding or Modifying the CES Search Application Pool Identity

By default, in IIS the CES search application pool runs with the NT AUTHORITY\NETWORK SERVICE system built-in identity. In certain cases, you may want to find or change the account under which the CES search application pool runs.
To find or modify the identity of the search application pool

1. Using an administrator account, connect to the Coveo Front-end server for which you want to find or modify the account used by the search application pool.

   **Note:** When setting up geographically distributed indexing (GDI), ensure to connect to the Coveo Front-end server of the local Coveo instance.

2. Start the Internet Information Services (IIS) manager, and then locate the CES search application pool identity:
   - For IIS 7:
     a. In the **Connections** panel, expand the server node and click **Application Pools**.
     b. On the **Application Pools** page, select the application pool for which you want to specify an identity, and then click **Advanced Settings** in the Actions pane.
     c. Under **Process Model**, select **Identity**, and then click the ... button to open the **Application Pool Identity** dialog box.

       In the **Application Pool Identity** dialog box, the CES search application pool account is identified by the selected option (either **Built-in account** or **Custom account**).
d. If you want to use a built-in account, select the **Built-in account** option and select an account from the [www.coveo.com](http://www.coveo.com).
list.

e. If you want to use a custom identity:
   i. Select the Custom account option, and then click Set.
   ii. In the Set Credentials dialog box, type the custom account name in the User name box, type a password in the Password box, retype the password in the Confirm password box, and then click OK.

f. Click OK to close the Application Pool Identity dialog box.

f. Click OK to close the Application Pool Identity dialog box.

   • For IIS 6:
     a. Expand the local computer.
     b. Find what is the application pool for the Coveo Enterprise Search 7 site:
        i. Expand Web Sites.
        ii. Right-click Coveo Enterprise Search 7, and then select Properties.
        iii. In the Coveo Enterprise Search 7 Properties dialog box, select the Home Directory tab.
iv. Read the CES search application pool in the **Application pool** parameter.

![Coveo Enterprise Search 6 Properties dialog box](image)

- **Local path:** C:\Program Files\Coveo Enterprise Search
- **Application name:** CESSearchApp
- **Starting point:** <Coveo Enterprise Search>
- **Execute permissions:** Scripts only
- **Application pool:** DefaultAppPool

C. Expand **Application Pools**.

D. Right-click the application pool found previously, and then click **Properties**.

E. Select the **Identity** tab to find the identity.

   In the **DefaultAppPool Properties** dialog box, the CES search application pool account is identified by the selected option under **Application pool identity** (either **Predefined** or **Configurable**).
To modify the identity, enter appropriate **User name** and **Password**, and then click **OK**.

**Note:** For a GDI configuration, the CES search application pool for the local Coveo instance must run under a domain account. It is a best practice to create a dedicated account for this purpose with a strong password that never changes.

11.3.3 Enabling Basic Authentication in IIS

You may need to enable basic authentication for the website hosting the Coveo search hubs.

To enable basic authentication in IIS 7

1. On the IIS server, start the IIS Manager (on the Windows taskbar, select **Start > Administrative Tools > Internet Information Services (IIS) Manager**).

2. In **Internet Information Services (IIS) Manager**:
   a. In the **Connections** panel, under **Sites**, select the site for which you want to enable basic authentication.

   **Example:** Select Coveo Enterprise Search 7.

   b. In the `<selected website> Home` page, in the center panel under **IIS**, double-click **Authentication**.
c. In the Authentication page, when Basic Authentication is set to Disable, right-click Basic Authentication, and then select Enable.

11.3.4 Enabling SSL in IIS

You may need to enable Secure Socket Layer (SSL) for the website hosting the search hubs.

To enable basic authentication in IIS 7

1. On the IIS server, start the IIS Manager (on the Windows taskbar, select Start > Administrative Tools > Internet Information Services (IIS) Manager).

   The Internet Information Services (IIS) Manager appears.

2. In the Connections panel on the left, under Sites, select the site for which you want to enable SSL.

   Example: Select Coveo .NET Front-End 12.

3. In the Actions panel on the right, under Edit Site, select Bindings.

4. In the Site Bindings dialog box:
   - When an HTTPS binding is already defined, click Close.
   OR
   a. Click Add.
   b. In the Add Site Binding dialog box:
      i. In Type, select https.
      ii. In SSL certificate, select an appropriate certificate from available choices.
iii. Click OK.

c. Click Close.

5. In the Connections panel on the left, under Sites, click the site again to display the <selected website> Home page.

6. In the <selected website> Home page in the center panel, under IIS, double-click SSL Settings.

7. In the SSL Settings page:
   a. Select the Require SSL check box.
   b. Under Client certificate, select Accept.

8. In the Actions panel on the right, click Apply to save your changes.

11.3.5 Enabling WebDAV in IIS

The WebDAV protocol is prohibited by default in IIS. When you want to use WebDAV for example for a Microsoft Exchange (WebDAV) source, you must allow WebDAV in IIS. This can be done from the Computer Management tool.

To enable WebDAV in IIS 6 on a Windows Server 2003

1. Using an administrator account, connect to the Windows server.

2. Open Computer Management (Start menu Administrative Tools > Computer Management).

3. In Computer Management:
a. In the navigation panel on the left, expand Services and Applications > Internet Information Services (IIS) Manager > Web Service Extensions.

b. In the panel on the right, click WebDAV, and then click Allow.

11.3.6 Resetting IIS

You may need to reset Microsoft Internet Information Services (IIS) while you perform configuration on a Coveo server or on a repository server.

To reset IIS

1. Using an administrator account, connect to the server on which you want to reset IIS.

2. Open the Windows Start menu and click Run.

3. In the Run dialog box that appears:
   a. In the Open box, type iisreset.
   b. Click OK.
Coveo Platform 7.0 | Administrator Guide

A DOS window temporarily appears to inform you that IIS is stopping and restarting.

11.4 Microsoft SQL Server
This section gathers topics related to the Microsoft SQL Server, which is a relational database management system
(see SQL Server). As a database, Microsoft SQL Server is a software product whose primary function is to store and
retrieve data as requested by other software applications such as the Coveo Platform 7. Microsoft SQL Server is
needed by the Coveo Usage Analytics module and the Coveo SharePoint web service (see "On-Premises Usage
Analytics Module" on page 649 and "Installing the Coveo Web Service, Search Box, and Search Interface into
SharePoint" on page 1309).

11.4.1 Creating a Database in Microsoft SQL Server
You may need to create a database in a Microsoft SQL Server, for example to create the database needed for the
Coveo Usage Analytics module.

To create a database in Microsoft SQL Server 2012
1. Connect to the computer where Microsoft SQL Server is installed using an administrator account.
2. Start Microsoft SQL Server Management Studio.
3. In the Connect to Server dialog box:
a. In Server type, select Database Engine.
b. In Server name, type or select the name of your SQL server instance in the form <hostname>\<SQL_

4www.coveo.com

88


instance_name>.

**Example**: On a server named *MyServer*, when using SQL Express with the default instance name, enter *MyServer\sqlexpress*.

c. In **Authentication**, select **Windows Authentication**.

d. Click **Connect**.

4. In **Microsoft SQL Server Management Studio**, in the **Object Explorer**, right-click on **Databases**, and then select **New Database** in the contextual menu.

5. In the **New Database** dialog box, in **Database name**, enter the desired database name, and then click **OK**.

**Example**: In the case of the Usage Analytics Module, enter the default Usage Analytics database name: *CoveoAnalytics*. You can use a different Usage Analytics database name, but you will need to specify this name in the *Web.config* file. Also, before running the database creation script, you will need to edit the first line of the database creation script to replace the default database name with the name you selected.
Coveo Platform 7.0 | Administrator Guide

To create a database in Microsoft SQL Server 2008
1. Connect to the Microsoft SQL Server computer using an administrator account.
2. Start Microsoft SQL Server Management Studio (on the Windows taskbar, select Start > All Programs >
Microsoft SQL Server 2008 > SQL Server Management Studio).
3. In the Connect to Server dialog box:
a. In Server type, select Database Engine.
b. In Server name, type or select the name of your SQL server instance in the form <hostname>\<SQL_
instance_name>.
Example: On a server named MySQLserver, when using SQL Express with the default instance name,
enter MySQLserver\sqlexpress.
c. In Authentication, select Windows Authentication.
d. Click Connect.

4www.coveo.com

90


4. In Microsoft SQL Server Management Studio, in the Object Explorer, right-click on Databases, and then select New Database in the contextual menu.

5. In the New Database dialog box, in Database name, enter the desired database name, and then click OK.

Example: In the case of the Usage Analytics module, enter the default Usage Analytics database name: CoveoAnalytics.
You can use a different Usage Analytics database name, but you will need to specify this name in the Web.config file. Also, before running the database creation script, you will need to edit the first line of the database creation script to replace the default database name with the name you selected.
11.4.2 Running a Script in Microsoft SQL Server

You may need to run a script in a Microsoft SQL Server for example to create the tables in the Coveo Analytics database.

To run a script in Microsoft SQL Server 2008

1. Connect to the Microsoft SQL Server computer using an administrator account.


3. In the Connect to Server dialog box, in Server name, select the name of your SQL server instance, and then click Connect.
4. In **Microsoft SQL Server Management Studio**, on the menu, select **File > Open > File**.

5. In the **Open File** dialog box, browse for the script file, and then click **OK**.

   **Example:** The Analytics database creation and migration scripts are available on the Coveo server in the [.NET_Front-End_Path]\Web\Analytics\Scripts\ folder.

6. On the SQL Editor toolbar, select the appropriate database, and then click **Execute** to run the script.

   ![SQL Editor](image)

   A message appears at the bottom of the **Microsoft SQL Server Management Studio** window to indicate that the execution of the script completed successfully.

   ![Query executed successfully.](image)

### 11.4.3 Adding the Microsoft SQL Server System Administrators Role

The CES administrative account must be a member of the Microsoft SQL Server system administrators server role when you want to install the Coveo SharePoint web service (see "Installing the Coveo Web Service, Search Box, and Search Interface into SharePoint" on page 1309).
The procedure applies to Microsoft SQL Server 2008, 2005, and 2000 but varies depending on the SQL Server version:

- "Microsoft SQL Server 2008 and 2005" on page 94
- "Microsoft SQL Server 2000" on page 95

11.4.3.1 Microsoft SQL Server 2008 and 2005

1. Access SQL Server Management Studio (Windows Start menu > All Programs > Microsoft SQL Server 2008 or Microsoft SQL Server 2005).

2. In the panel on the left, expand localhost > Security, and then click the Logins node.

3. When the login for the CES administrative account already exists, double-click it. Otherwise, right-click Logins, and then click New Login.

4. In the Login - New dialog box:
   a. In the Login Name box, enter the CES administrative account.
   b. In the panel on the left, click Server Roles.
   c. In the panel on the right, in the Server roles list, select sysadmin.
11.4.3.2 Microsoft SQL Server 2000

1. Access SQL Server Enterprise Manager (Windows Start menu > All Programs > Microsoft SQL Server).
2. In the panel on the left, expand Microsoft SQL Servers > SQL Server Group > [your server group] > Security.
3. Click the Logins node.
4. When the login for the CES administrative account already exists, double-click it. Otherwise, right-click Logins, and then click New Login.
5. In the SQL Server Login Properties - New Login dialog box:
   a. In the Login Name box, enter the CES administrative account.
   b. Click the Server Roles tab.
c. In the **Server Role** list, select **System Administrators**.

d. Click **OK**.

### 11.4.4 Adding the Database Owner Role for Microsoft SQL Server

You need to add the CES administrative account to the database owner role for Microsoft SQL Server when you want to install the Coveo SharePoint web service (see "Installing the Coveo Web Service, Search Box, and Search Interface into SharePoint" on page 1309).

The procedure applies to Microsoft SQL Server 2008, 2005, and 2000, but varies depending on the SQL Server version:

- "Microsoft SQL Server 2008/2005" on page 96
- "Microsoft SQL Server 2000" on page 98

#### 11.4.4.1 Microsoft SQL Server 2008/2005

1. Access **SQL Server Management Studio** (Windows Start menu > All Programs > Microsoft SQL Server 2008 or Microsoft SQL Server 2005).

2. Connect to the appropriate database.
3. In the panel on the left, expand localhost > Security > Logins.

4. When the login for the CES administrative account already exists, double-click it. Otherwise, right-click Logins, and then click New Login.

5. In the Login - New dialog box:
   a. In the Login Name box, type the CES administrative account.
   b. In the panel on the left, click User Mapping.
   c. In the panel on the right:
      i. In the Users mapped to this login list, in the Map column, select the check box for the database to which you want to assign the owner role to the CES administrative account.
      ii. In the Database role membership for list, select db_owner.
   d. Click OK.
11.4.4.2 Microsoft SQL Server 2000

1. Access **SQL Server Enterprise Manager** (Windows Start menu > All Programs > Microsoft SQL Server).

2. In the panel on the left, expand **Microsoft SQL Servers** > **SQL Server Group** > [your server group] > **Security**.

3. Click the **Logins** node.

4. When the login for the CES administrative account already exists, double-click it. Otherwise, right-click **Logins**, and then click **New Login**.

5. In the **SQL Server Login Properties - New Login** dialog box:
   a. In the Login Name box, type the CES administrative account.
   b. Click the **Database Access** tab.
   c. In the list at the top, in the Permit column, select the check box for the database to which you want to assign the owner role for the CES administrative account.
   d. In the Permit in Database Role list, select **db_owner**.
   e. Click **OK**.
11.5 Microsoft SharePoint

This section gathers topics related to procedures that you may need to perform in your SharePoint farm to properly configure the crawling account for the Coveo connector for Microsoft SharePoint (see "Microsoft SharePoint Connector" on page 1243).

11.5.1 Adding the Full Read Policy to All SharePoint Farm Web Applications

You must add the Full Read policy to all SharePoint farm web applications for the crawling account when you want to perform SharePoint content and security indexing, incremental refresh, and site collection discovery.

The procedure applies to SharePoint 2013, 2010, and 2007 and varies depending on the SharePoint version:

- "Microsoft SharePoint 2013 or 2010" on page 99
- "Microsoft SharePoint 2007" on page 100

Note: The permissions required for the crawling account in the case of SharePoint Online are different.

11.5.1.1 Microsoft SharePoint 2013 or 2010


2. In SharePoint 2013/2010 Central Administration, under Application Management, click Manage web applications.

3. For each web application to crawl:
   a. In the Web Applications Management page:
      i. Click the name of the desired web application to highlight it.
      ii. In the ribbon, click User Policy.
   b. In the Policy for Web Application dialog box, click Add Users.
   c. In the Add Users wizard:
i. In the Zone drop-down list, select (All zones), and then click Next.

ii. In the Users text box, add the crawling account.

iii. Under Permissions, select the Full Read - Has full read-only access check box.

iv. Click Finish.

d. In the Policy for Web Application dialog box, click OK.

11.5.1.2 Microsoft SharePoint 2007

1. Access SharePoint 3.0 Central Administration (Windows Start menu > All Programs > Microsoft Office Server).

2. Click Application Management.

3. Click Policy for Web application.

4. For every web application to crawl:
   a. Click Add Users.
   b. Select (All Zones), and then click Next.
   c. In the Users text box, add the crawling account.
d. Under Permissions, select the Full Read - Has full read-only access checkbox, and then click Finish.

11.5.2 Adding the SharePoint Website Read Permission

You must add the SharePoint site Read permission to the crawling account when you want to:

- Perform SharePoint personal site and user profile indexing.
- Take advantage of the automatic permission setup feature of the SharePoint connector (see "Automatic Permissions Setup" on page 1307).

The procedure applies to SharePoint 2013, 2010, and 2007 and varies depending on the SharePoint version:

- "Microsoft SharePoint 2013 or 2010" on page 101
- "Microsoft SharePoint 2007" on page 102

11.5.2.1 Microsoft SharePoint 2013 or 2010

1. Access the SharePoint site collection that you want to index.
2. Click the gear icon (SharePoint 2013) or the Site Actions (SharePoint 2010), and then select Site Permissions.
3. In the ribbon, click Grant Permissions.
4. In the Grant Permissions dialog box:
a. In the Users/Groups text box, add the crawling account.

b. Under Grant Permissions, select the Grant users permission directly radio button, and then select the Read - Can view pages and list items and download documents check box.

c. Click OK.

11.5.2.2 Microsoft SharePoint 2007

1. Access the SharePoint site collection site collection that you want to index.

2. Click Site Actions, and then select Site Settings.

3. Click Advanced Permissions in the Users and Permissions column.

4. Click New.

5. In the Add Users page:
11.5.3 Adding the Retrieve People Data for Search Crawlers Permission to the User Profile Service Application

You must add the Retrieve People Data for Search Crawlers permission to the User Profile Service application for the crawling account when you want to perform SharePoint personal site and user profile indexing. This procedure applies only to SharePoint 2013 and 2010.

To add the Retrieve People Data for Search Crawlers permission to the User Profile Service application


2. In the SharePoint 2013/2010 Central Administration, under Application Management, click Manage service applications.

3. In the Manage Service Applications page:

   a. In the Users/Groups text box, add the crawling account.

   b. Under Give Permission, select the Give users permission directly radio button, and then select the Read - can view only check box.

   c. Click OK.

www.coveo.com

103
a. Without clicking it, highlight **User Profile Service Application**.

**Note:** When **User Profile Service Application** is not present in the service applications list, the **User Profile Service Application** may not be installed on your SharePoint farm, and there is therefore no people data to index. Abort this procedure.

b. In the ribbon, click **Administrators**.

4. In the **Administrators for User Profile Service Application** dialog box:
a. In the first box, type the crawling account, and then click **Add**.

b. In the second box, select the crawling account.

c. In the **Permission for Administrators** list, select the **Retrieve People Data for Search Crawlers** check box, and then click **OK**.

11.5.4 Adding the Manage User Profiles Permission in Shared Service Rights

You must add the **Manage user profiles** to **Shared Service Rights** for the crawling account when you want to index SharePoint personal sites and user profiles. This procedure applies only to MOSS 2007 (SharePoint 2007).

To add the Manage user profiles permission to Shared Service Rights

1. Access SharePoint 3.0 **Central Administration** (Windows **Start** menu > **All Programs** > **Microsoft Office Server**).

2. Click **Shared Services Administration**.

3. Click the shared service link hosting the user profiles and personal sites data.

4. Click **Personalization service permissions**.

5. Click **Add Users/Groups**.

6. In the **Add Users/Groups: Shared Service Rights** page:

   a. In the **Users/Groups** text box, add the crawling account.

   b. In the **Choose Permissions** section, select the **Manage user profiles** check box.

   c. Click **Save**.

11.5.5 Adding the Crawling Account to the SharePoint Farm Administrators Group

You must add the crawling account to the SharePoint farm administrators group when you want to:
- Install the Coveo SharePoint web service (see "Installing the Coveo Web Service, Search Box, and Search Interface into SharePoint" on page 1309).

- Take advantage of the automatic permissions setup feature of the SharePoint connector (see "Automatic Permissions Setup" on page 1307).

The procedure varies depending on the SharePoint version:

- "Microsoft SharePoint 2013" on page 106
- "Microsoft SharePoint 2010" on page 107
- "Microsoft SharePoint 2007" on page 108

11.5.5.1 Microsoft SharePoint 2013

1. Access SharePoint 2013 Central Administration (Windows Start menu > All Programs > Microsoft SharePoint 2013 Products).

2. In the SharePoint Central Administration:
   a. In the Central Administration menu on the left, select Security.
   b. In the Security page, under Users, click Manage the farm administrators group.
   c. In the People and Groups - Farm Administrators page, click New.
   d. In the Share 'Central Administration' dialog box, in the Add people to the Farm Administrators group
box, add the crawling account, and then click **Share**.

### 11.5.5.2 Microsoft SharePoint 2010

1. Access **SharePoint 2010 Central Administration** (Windows **Start** menu > **All Programs** > **Microsoft SharePoint 2010 Products**).

2. In **SharePoint 2010 Central Administration**, under **Security**, select **Manage the farm administrators group**.

3. In the **People and Groups** page, click **New**.
4. In the **Grant Permissions** dialog box, in the **Users/Groups** box, add the crawling account, and then click **OK**.

11.5.5.3 Microsoft SharePoint 2007

1. Access SharePoint 3.0 **Central Administration** (Windows Start menu > All Programs > Microsoft Office Server).

2. Click **Operations**.

3. Click **Update farm administrator's group**.

4. Click **New**.

5. In the **Add Users** page:
11.5.6 Finding the Assembly Type of a SharePoint Web Part

You may need to find the assembly type of Web Parts that you want to index when you select the **Index the content of the WebParts of these types only** option for a SharePoint source.

**Tip:** When useful, you can also get SharePoint Web Part assembly name and type programmatically (see Get web part assembly name and type name from SharePoint web part gallery).

To find the assembly type of a SharePoint Web Part

1. Using a SharePoint administrator account, select the site collection containing the Web Part that you want to index.
2. In the **Site Actions** menu, select **Site Settings**.
3. In the **Site Settings** page, under **Galleries**, click **Web Parts**.
4. In the list of Web Parts that appears, click the Edit icon for the Web Part that you want to index.

The Web Part file can either have a `.dwp` or a `.webpart` extension.
Example: Click the Edit icon for the MSContent Editor.dwp file corresponding to the default Web Part assembly type.

5. Click View XML.

6. In the XML, copy the text between the <TypeName> and </TypeName> tags.

Example: In the following XML code, you would copy Microsoft.SharePoint.WebPartPages.ContentEditorWebPart.

```xml
<?xml version="1.0" encoding="utf-8"?>
<WebPart xmlns="http://schemas.microsoft.com/WebPart/v2">
  <Assembly>Microsoft.SharePoint, Version=12.0.0.0, Culture=neutral, PublicKeyToken=71e9bce11e9429c</Assembly>
  <TypeName>Microsoft.SharePoint.WebPartPages.ContentEditorWebPart</TypeName>
  <Title>Content Editor Web Part</Title>
  <Description>Use for formatted text, tables, and images.</Description>
  <PartImageLarge>/_layouts/images/mscontl.gif</PartImageLarge>
</WebPart>
```

11.5.7 Finding the Enabled Claims Authentication Type for a SharePoint Web Application

You may need to identify the Claims authentication type that is enabled for a SharePoint Web Application when you create a security provider.

To find the enabled Claims authentication type in a SharePoint 2013/2010 Web Application


2. In SharePoint 2013/2010 Central Administration, under Application Management, select Manage web applications.

3. Select the Web Application for which you want to find the Claims authentication type, and then click Authentication Providers.

4. Click on the name of the Zone using Claims Based Authentication.

5. Scroll down to the Claims Authentication Types section.

11.5.8 Finding and Enabling the ADFS Service Endpoint URL Path

You may need to find and ensure that the Active Directory Federation Services (ADFS) service endpoint URL path is enabled when you create a Claims security provider.

To find and enable the ADFS service endpoint URL path

1. Access AD FS 2.0 Management Console (Windows Start menu > All Programs > Administrative Tools > AD FS 2.0 Management).

2. In AD FS 2.0 Management Console, under Services, select Endpoints.

3. Find the endpoint by looking at the Url Path column.

4. When the endpoint is disabled, right-click it, and then select Enable.
11.5.9 Finding Your Office 365 Native Domain Name
You may need to find the native domain name associated with your Office 365 account when you create a SharePoint Online security provider.

To find the native domain name associated with your Office 365 account

1. Log on to the Microsoft Office 365 Online Portal using an administrative account.
2. Under Management, click on Domains.
3. The native domain should be listed with a name ending with .onmicrosoft.com.

11.5.10 Finding the Relying Party Trust Identifier for a SharePoint Web Application
You may need to find the Relying Party Trust identifier for your SharePoint Web Application when you create a Claims security provider.

To find the Relying Party Trust identifier for your SharePoint Web Application

1. Access AD FS 2.0 Management Console (Windows Start menu > All Programs > Administrative Tools > AD FS 2.0 Management).
2. In AD FS 2.0 Management Console, under Trust Relationships, select Relying Party Trusts.
3. In the Relying Party Trusts list:
   a. For an on-premises SharePoint, find the line for SharePoint. The ADFS Relying Party Identifier will be the value in the Identifier column.
   b. For SharePoint Online, the ADFS Relying Party Identifier is typically urn:federation:MicrosoftOnline, but you can validate it as follows:
      a. Right-click the Microsoft Office 365 Identity Platform line, and then select Properties.
      b. In the Microsoft Office 365 Identity Platform Properties dialog box, select the Identifiers tab.
      c. In the Relying party identifiers list, the ADFS Relying Party Identifier is the one starting with urn:;
11.5.11 Finding the Relying Party Trust Identifier for a SharePoint ADFS server

You may need to find the Relying Party Trust identifier for your SharePoint ADFS server when you create a Claims security provider.

Some federation environments use multiple ADFS servers to authenticate users in SharePoint. In these environments, a trust is established between SharePoint and an ADFS server, and another trust between this ADFS server and another ADFS server. Configurations using multiple ADFS servers can be used, for example, when federating users from different Active Directory domains.

In order for the Claims security provider to be able to authenticate to SharePoint web applications using such a configuration, information from both ADFS servers is required.

To find the Relying Party Trust identifier for your SharePoint ADFS server

1. Log on to the ADFS server which is trusted by the SharePoint ADFS server.

2. Access **AD FS 2.0 Management Console** (Windows **Start** menu > **All Programs** > **Administrative Tools** > **AD FS 2.0 Management**).

3. In **AD FS 2.0 Management Console**, under **Trust Relationships**, select **Relying Party Trusts**.
4. In the list of trusts displayed, find the trust for the ADFS server which is trusted by SharePoint. The ADFS Relying Party Identifier will be the value in the Identifier column.

11.5.12 Granting the Site Collection Administrator Permission in SharePoint Online

In SharePoint Online, the CES crawling account must be an administrator in Office 365 (CES 7.0.7914+ (October 2015)) and an administrator of all SharePoint Online site collections from which you want to index content, but also the root site collection.

This high level permission is required because SharePoint Online currently does not offer lower level permissions that allow to crawl site collection content. The root site collection administrator permission is needed by the SharePoint auto discovery mechanism that the Coveo connector uses for operations such as detecting refreshed and deleted folders and crawling.

Grant the administrator permission using SharePoint Online admin center

2. Click Manage site collections.
3. In the navigation panel on left, click Site Collections.
4. In the panel on the right, under Site Collections, select one or more site collections you want to crawl.
5. In the tool bar, click Owners, and then Manage Administrators.
6. Add the crawling account to the list of Site Collection Administrators.
7. Click OK.

What's Next?

Assign the admin role to your crawling account in Office 365 (see Assigning admin roles in Office 365).

11.5.13 Adding the Personal Sites Collections Owner Permissions for SharePoint Online

You must make the crawling account an owner of all the personal sites collections when you want to index SharePoint Online personal sites and user profiles. The crawler will only be able to index content from a personal
site if the crawling account is an owner of this personal site, other personal sites for which it is not an owner will be ignored.

You can add these permissions using one of the following methods:

- **Using the admin center (SharePoint Online 2010 and 2013)**

  SharePoint Online admin center allows granting owner permissions for only one personal site collection at a time, which means this procedure has to be done for every personal site collection.

- **Using a PowerShell script (SharePoint Online 2013 only)**

  A PowerShell script using SharePoint Online cmdlets is available to facilitate the task of granting owner permissions to a specific account for all personal site collections.

To add the Owner permission using SharePoint Online admin center

1. Access **SharePoint Online administration center** (https://your_domain-admin.sharepoint.com).
2. In the navigation panel on the left, click **user profiles**.
3. Click **Manage User Profiles**.
4. Use the search box to find the user profiles of the users you want to crawl.
5. Right-click an Account Name and then select **Manage site collection owners**.
6. Add the crawling account to the list of **Site Collection Administrators**.
To grant the Owner permission using SharePoint Online Management Shell

Notes:

- You must regularly perform the following procedure when you want to grant permissions for site collections of new users.
- This procedure applies to SharePoint Online only.

1. Install SharePoint Online management shell (see the Microsoft document Set up the SharePoint Online Management Shell Windows PowerShell environment).

2. Download the zipped COVEOSPO.ps1 script file to the server where the SharePoint Online management shell was previously installed.

   **Important:** The script was updated on January 21, 2016.

3. Unzip the file.

4. On the Windows menu select **Start > All Programs > SharePoint Online Management Shell.**

5. Load the COVEOSPO.ps1 script.
6. Run the `Set-COVEOSPOMySitesOwner` and `Set-COVEOSPOSitesAdmin` cmdlets.

The following table lists the parameters supported by each of the cmdlets:

<table>
<thead>
<tr>
<th>Parameter and definition</th>
<th>Set-COVEOSPOMySitesOwner</th>
<th>Set-COVEOSPOSitesAdmin</th>
</tr>
</thead>
<tbody>
<tr>
<td>AdminSiteUrl</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td><strong>Specifies the URL of the SharePoint Online tenant.</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>AdminUsername</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td><strong>Specifies the username of the SharePoint Online global administrator used to connect to the SharePoint server. This user will be added to the sites collection administrators (for the <code>Set-COVEOSPOMySitesOwner</code> cmdlet) or the personal sites administrators (for the <code>Set-COVEOSPOSitesAdmin</code> cmdlet) if the <code>NewAdminUsername</code> parameter is empty.</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>AdminPassword</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td><strong>Specifies the password of the SharePoint Online global administrator used to connect to the SharePoint server.</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>UsersDomainName</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td><strong>Specifies the domain of the users from which to retrieve personal sites.</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>NewAdminUsername</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td><strong>Specifies the username of one or more SharePoint Online users and/or group(s) to be added in the sites collection administrators (for the <code>Set-COVEOSPOMySitesOwner</code> cmdlet) or the personal sites administrators (for the <code>Set-COVEOSPOSitesAdmin</code> cmdlet). If not set, the user specified in the <code>AdminUsername</code> parameter will be added.</strong></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Notes:**
- You can add user and group at the same time by separating values with comma.
- **Example:** `-NewAdminUsername "user1@domain.com","user2@domain.com","c:0-f\rolemanager\s-{accountNumber}"`
- You must find the group ID to add the associated users in the sites collection or personal sites administrators (see To find a SharePoint group ID).

**Remove**

This parameter is a switch that, when included in the script, removes the user(s) and/or group(s) specified in the `NewAdminUsername` parameter (instead of adding them) from the sites collection administrators (for the `Set-COVEOSPOMySitesOwner` cmdlet) or the personal sites administrators (for the `Set-COVEOSPOSitesAdmin` cmdlet).
Examples:

- `Set-COVEOSPOMySitesOwner -AdminSiteUrl https://acme-admin.sharepoint.com -AdminUsername admin@acme.onmicrosoft.com -AdminPassword password -UsersDomainName acme.onmicrosoft.com`

- `Set-COVEOSPOSitesAdmin -AdminSiteUrl https://acme-admin.sharepoint.com -AdminUsername globaladmin@acme.onmicrosoft.com -AdminPassword password -NewAdminUsername "user@acme.onmicrosoft.com", "c:0-f|rolemanager|s-21-2644810858-3409521387-2709630237-4818302"`

To find a SharePoint group ID

1. If not already done, repeat the procedure to add the Owner permission using SharePoint Online admin center to the group, but without performing the last step.

2. In the site collection owners panel, access the source code of the page by pressing F12 or by right-clicking, and then selecting Inspect (Google Chrome) or View Page Source (Firefox).

3. In the window that appears, in the source code, prior to `displaytext='GroupName'`, copy the value of the key parameter (key='GroupID').

You can now paste the group ID in the NewAdminUsername parameter to add/remove the group members in/from the sites collection or personal sites administrators.

11.6 Microsoft Windows Server

This section presents a procedure that you may need to perform, on two particular situations, in your SharePoint farm to properly configure the Coveo connector for Microsoft SharePoint (see "Microsoft SharePoint Connector" on page 1243 and "Adding the Crawling Account to the SharePoint Server Local Administrators Group" on page 118).
11.6.1 Adding the Crawling Account to the SharePoint Server Local Administrators Group

You may need to add the crawling account to the SharePoint server local Administrators group when you want to:

- Perform SharePoint personal site and user profile indexing, incremental refresh, and site collection discovery (see "Granting SharePoint Permissions to the Crawling Account" on page 1307).
- Install the Coveo SharePoint web service (see "Installing the Coveo Web Service, Search Box, and Search Interface into SharePoint" on page 1309).

Note: This procedure applies to Microsoft Windows Server 2008.

To add the crawling account to the SharePoint server local administrator group

1. On the SharePoint server, access the Computer Management console (Windows Start menu > All Programs > Administrative Tools).
2. In the panel on the left, expand System Tools > Local Users and Groups, and then click Groups.
3. In the panel on the right, right-click Administrators, and then click Add to Group.
4. In the Administrators Properties dialog box:
   a. Click Add.
   b. In the Select Users, Computers, or Groups dialog box, enter the crawling account, and then click OK.
   a. Click OK to close the Administrators Properties dialog box.

11.7 Changing the RabbitMQ Administrator Password

Coveo Enterprise Search (CES) installs RabbitMQ that is needed to operate with other Coveo products such as Coveo for Sitecore. The CES installation wizard offers and recommends to set the RabbitMQ administrator credentials (see Installing CES on the Master Server).

The following procedure describes how to change the RabbitMQ administrator password when RabbitMQ is already installed.
To change the RabbitMQ administrator password

1. Using an administrator account, connect to the server where CES is installed.

2. Using a browser on the server, access the http://localhost:15672/ URL, and then enter the current administrator credentials.

3. In the RabbitMQ Management page:
   a. On the navigation toolbar at the top, click Admin.
   b. In the navigation panel on the right, click Users.
   c. Under Users, click the administrator user.
   d. Click Update this user to expand the section.

Note: The default administrator username and password are guest and guest.
e. Next to Password, enter the new password twice, and then click Update user.

4. Take a note of these credentials in a safe place of your choice.
12. CES Performance

The Coveo Administration Tool provides multiple ways to improve the performance of CES, such as the customization of index options and the configuration of stop words often diluting the important terms in a query.

12.1 Limiting the Size of the Coveo index

CES is designed to help organizations index millions of documents. When the disk space is limited, you can customize CES to index only pertinent information (ex.: the roots of words) while leaving out non-essential data (ex.: plural variations of words)—because each organization has different requirements, the index options can be fully customized. Moreover, CES proposes maintenance tools to keep the index as compact as possible.

**Note:** The Coveo Platform 7 features a self-optimizing index that no longer needs scheduling index optimization tasks (see "About the Index Self-Optimization Process" on page 270).

The following table describes different actions that you can take in the Administration Tool to limit the index size.

<table>
<thead>
<tr>
<th>Where</th>
<th>What</th>
<th>How</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Add Source page</strong>&lt;br&gt;Index &gt; Sources and Collections page &gt; Sources section, click Add to get to the Add Source page (see &quot;Adding a Source&quot; on page 281).</td>
<td>When indexing Local/Network Files, SharePoint, Documentum, Exchange Crawler, Enterprise Vault or ODBC sources, do not index subfolders or subsites.</td>
<td>1. In the Source Type drop-down list, select the appropriate source type.&lt;br&gt;2. In the Options section, clear the Index subfolders check box.&lt;br&gt;3. Complete the indexing of the source (see &quot;Adding a Source&quot; on page 281).</td>
</tr>
<tr>
<td><strong>Filters page</strong>&lt;br&gt;1. Access the Sources and Collections page (Index &gt; Sources and Collections).&lt;br&gt;2. In the Sources section, expand the appropriate source drop-down list.&lt;br&gt;3. Select Edit Filters.</td>
<td>Add exclusion filters to exclude documents that do not need to be indexed.</td>
<td>1. Click Add an Exclusion Filter.&lt;br&gt;2. In the Excluded Pattern box, enter the addresses of the documents to exclude (one entry per line, use wildcards if necessary).&lt;br&gt;3. Click Save. (see &quot;Adding or Modifying Source Filters&quot; on page 295)</td>
</tr>
</tbody>
</table>
### Where

**Advanced** page of Web sources
1. Access the **Sources and Collections** page (Index > Sources and Collections).
2. In the **Sources** section, expand the appropriate Web source drop-down list.
3. Select **Edit Advanced**.

### What

Restrict crawling to one (only the main page) or two (the main page and pages directly linked to it) levels.

### How

1. In the **Crawling** section, select **Restrict crawling to X levels** and enter the appropriate number of level (see "Modifying Advanced Source Parameters" on page 305).

### Query History page (Reports > Query History) or Index History page (Reports > Index History)

Export the reports to Excel, and then delete the repost history on the Coveo server.

### How

1. In the **Fixed** drop-down list, select the appropriate time period.
2. Click **Update**. The report appears.
3. Click **Export**. The **File Download** box appears.
4. Click **Save**.
5. Access the **Settings** page (Reports > Settings).
6. In the **Index History** or **Query History** section, beside **Delete index history older than** or **Delete query history older than** select the appropriate date (in order to delete only the exported reports).
7. Click **Delete index history older than** or **Delete query history older than**.

### Setting page (Logs > Settings)

Keep logs for less than 90 days.

### How

1. In the **Log Archive** section, select the **Keep logs for the last X days** option and enter the appropriate number of days.

### Languages page

Access the **Converter Managers** page (Configuration > Converters) and click **Languages** in the navigation panel on the left.

Do not index documents if their language is not recognized by CES.

### How

1. In the **Language Detection** section, select **Reject the document** (see "Modifying How Documents Written in Unrecognized Languages Are Indexed" on page 468).

### 12.2 Speeding up CES

CES is designed to function properly on servers complying with the minimum system requirements (see "Coveo Platform Hardware and Software Requirements" on page 3). However, when processes other than CES are running in parallel or a large number of users are querying the index on a regular basis, the Coveo server can be slowed down.
Note: It is recommended to distribute the indexing and querying processes over the day by indexing and refreshing documents during off-hours when few queries are made.

The following table describes different actions that you can take using the Administration Tool to keep CES running at maximum speed.

<table>
<thead>
<tr>
<th>Where</th>
<th>What</th>
<th>How</th>
</tr>
</thead>
<tbody>
<tr>
<td>Status &gt; Details page</td>
<td>Disable queries to speed up indexing or vice versa.</td>
<td>In the System State section, click Disable beside Queries are enabled or Indexing is enabled.</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Note:</strong> In order to re-enable the process, click Enable.</td>
</tr>
</tbody>
</table>
| General page of sources      | Disable document summarization to save CPU resources during indexing.  | 1. Select Index > Sources and Collections.  
2. In the Sources section, expand the appropriate source drop-down list.  
4. In the Options section, select Disable document summarization (see "Modifying General Source Parameters" on page 292). |
| Advanced page of sources     | Disable advanced text layout analysis for PDF documents and advanced duplicate document filtering in order to speed up indexing.    | 1. Select Index > Sources and Collections.  
2. In the Sources section, expand the appropriate source drop-down list.  
3. Select Edit Advanced.  
4. In the Performance section, select Disable advanced text layout analysis for PDF documents and Disable advanced duplicate document filtering (see "Modifying General Source Parameters" on page 292). |
Perform extra ranking process on fewer than 100 results to speed up querying. In the Optimization section, enter the appropriate number of documents submitted to the extra ranking process.

Increase the size of the memory cache available to CES processes to speed up indexing and querying. In the Memory cache size box, enter the appropriate number of MB available.

Select the appropriate Performance Mode option for the process that you want to improve. In the Performance Mode section, select the appropriate option (see "Modifying or Using Advanced Index Parameters" on page 366).

Example: During the initial indexing, you may want to select the Optimize for indexing option, and when completed, select the Optimize for querying option if you want to favor the query process.

When the number of documents in one slice reaches the recommended limit, add another slice to distribute the index content and, therefore, speed up indexing and querying. See "Coveo Platform Hardware and Software Requirements" on page 3 and "Adding an Index Slice to the Master Server" on page 342

Note: Adding more slices than needed can actually degrade performances.

Configure new mirrors in order to distribute queries between indexes and, therefore, speed up querying. See "Adding a Mirror Server" on page 338

Set the priority of the main process to Highest or Above Normal to prioritize CES over other processes running on the server. In the Main process priority drop-down list, select Highest or Above Normal.

Note: You can also prioritize indexing or crawling over other processes; however, doing so slows down queries.

12.3 Configuring the Index to Ignore Stop Words in Queries

Note: With a Coveo Cloud Organization, you can configure stop words in the query pipeline (see Managing Query Pipeline Stop Words).

CES 7.0.4887+ (November 2012)

The Coveo Platform 7 indexes all terms contained in documents, including short very common words known as stop words (such as: a, the, a, at, by, for, in, it, of, to, the, this, that,…). Indexing these short words allows users to search and find exact occurrences of phrases.
However, sometimes considering short common words present in a query may dilute the important terms and reduce the relevance of the search results. You can configure CES to ignore a custom list of stop words at query time to improve search results relevance for natural language type of queries.

**Example:** A user enters the following natural language query:

How do I change my password in the intranet

The stop words (such as do, I, my, in, and the) may contribute to return search results not relevant to the main terms of the query (how, change, password, and intranet).

When you include these terms in a custom stop word list, the query sent to the index is:

How change password intranet

The terms in the custom stop word list are considered except in the following cases:

- Stop words within a phrase search.
- A stop word is an argument of the **NOT** or **NEAR** operators.
- The query contains only stop words.

You must contact Coveo Support for instructions to get instructions to configure stop words to ignore in queries.
13. Coveo Platform Troubleshooting Guide

Issues with the Coveo Platform can be broken down into four main categories:

- "CES Service" on page 126
- "Crawling" on page 127
- "Performance" on page 128
- "Search Interface" on page 129

Each category can be further broken down into different types of problems for which Coveo Support may require different files to properly assist in troubleshooting.

This topic gives you an overview where to look for the source of any problem and what information you should send to Coveo Support to assist you in this troubleshooting.

13.1 CES Service

CES Service Outage

A CES service outage occurs when the CESServiceX.exe process (CESMirrorServiceX.exe on mirror server) stops unexpectedly.

Symptoms:

- No access to the Administration Tool
- The Back-End server does not respond to queries.
- In the case of a main server, crawling stops.
- In almost all cases, core dump files are created to help Coveo Support understand the cause of the issue.

What you should provide to Coveo Support for assistance on this type of issue:

1. A copy of the .dmp and .txt files from the \[CES_Path\]\CoreDumps folder.

2. The output of the SystemStatus tool running the number 2 option (see "Using the Coveo SystemStatus Tool" on page 131).

3. Analysis or troubleshooting details that you have already done.

CES Service Hang

Symptoms:

- The Administration Tool does not load
- The search interface does not load
- The normal crawling schedules does not start.
- In all cases the CES service always appears to be running normally.
Usually restarting the service resolves the issue, but to ensure that information on the problem is not lost, when possible this should not be done until instructed by Coveo Support.

What you should send to Coveo Support for assistance on this type of issue:

- The output of the SystemStatus tool running the number 3 option (see "Using the Coveo SystemStatus Tool" on page 131).

13.2 Crawling

Index in Read-Only Mode

Symptoms:

- All crawling is stopped
- All Administration Tool controls are disabled (grayed out).

Possible causes:

1. A schedule toggled the index in read-only mode between certain hours.
   
   You can verify schedules from the Administration Tool (see "Modifying System Schedules" on page 439).

2. Someone manually toggled the index in read-only mode.
   
   The system logs all actions performed in the Administration Tool and who was logged in at the time (found in [Index_Path]\Logs\) so you can find out who switched the index to read-only mode.

3. Low disk space automatically switches the index to read-only mode.
   
   This is also recorded in system logs. When email alerts are configured to Error level, an email alert will be sent out when this happens (see "Configuring Email Alerts" on page 528).

Crawling Stops Before it Should or Crawling Won't Start at All

This problem is usually accompanied by a message in the Index logs with the ERROR level that explains why the crawling stopped or wouldn’t start (found in [Index_Path]\Logs\).

What you should provide to Coveo Support for assistance on this type of issue:

1. The index logs from the time when the problem occurred found in the [drive]\CES7\Logs\ folder.

2. The Coveo config.txt file found in the [Index_Path]\Logs\ folder.

3. The name of the collection and source that is affected.

4. Any mapping or configuration file referenced in the source.

Crawling Completes but Some Documents Can't Be Found

Possible causes and related symptoms:

1. A document is indexed but its content can’t be found
   
   From the search interface, you can find the document using its file name but not using any of its content.
In this case, the document is most likely indexed by reference. When a document is indexed by reference only its path and basic metadata is indexed, the content is not (see "What Is the Difference between Indexing by Reference and Indexing by Content?" on page 481).

Two things you can check:

a. In the Administration Tool, ensure that the Action for the type of this document is set to Index entire document (see "Modifying How CES Handles a Document Type" on page 477).

b. Look in the index logs for the document in question (found in [Index_Path]\Logs\). You should find an entry with a WARNING level that has an error message explaining why the document was indexed by reference.

2. A document is indexed but it can’t be found

Security is the most likely culprit if the document has been indexed but can’t be found from the search interface:

- Using the Index Browser, find the document and compare the security that is on the document in the index and ensure that it matches the security on the document in its original repository (see "Reviewing Document Details from the Index Browser" on page 375).

- If everything looks fine there, you can then check the security that the search interface detects for a user that should find the document by adding debug=1 to the query string. This information can be provide to Coveo Support for analysis.

13.3 Performance

Transactions Are Slow to Apply to the Index

The most common cause of slow transaction application to the index is I/O related because this process can be very disk intensive.

To gather troubleshooting information:


- Enable trace logging for the transaction to see exactly which action causes the bottle neck (see "Using Transaction Trace Logging" on page 138).

What you should send to Coveo Support for assistance on this type of issue once the logging is disabled:

1. Results of the Windows Performance Monitor.

2. The output of the SystemStatus tool running the number 2 option (see "Using the Coveo SystemStatus Tool" on page 131).

3. The output of the transaction trace logs (the [Index_Path]\Index\Default\Default\CESProfiling- Trn*.txt files from each slice).

Queries Are Slow

In general, you should expect a Coveo search interface to return search results for a query in less than one
second. Special cases like a modified search page that launches several sub queries or wildcard queries are generally expected to take longer.

When queries take longer than expected, check the following:

1. On the Coveo Master server, using the Task Manager, check to see if all server CPUs are consistently at 100% usage.

2. Does the server meet the Coveo recommended system requirements (see "Coveo Platform Hardware and Software Requirements" on page 3)?

3. Is Coveo running on a dedicated server? If not the server specs should be increased to take the extra load into consideration.

4. How many queries does the server receive (see "What Information Is Displayed in the Query History?" on page 386)? If you have more, consider adding a Coveo Mirror server to distribute the load (see "Adding a Mirror Server" on page 338).

What you should provide to Coveo Support for assistance on this type of issue:

1. Query profiling files (see "Using Query Profiling" on page 138).

2. Results of the Windows Performance Monitor while the query profiling is enabled (see "Gathering Windows Server Performance Monitor Information" on page 135).

3. The output of the SystemStatus tool running the number 2 option once the profiling run is done (see "Using the Coveo SystemStatus Tool" on page 131).

13.4 Search Interface

Generally, search interface issues can be broken down into two categories:

- Problems in the skin
- Problems with the search interface settings

What you should provide to Coveo Support for assistance on this type of issue:

1. The name of the search interface that has the problem

2. A zip file of the [.NET_Front-End_Path]\Web\Coveo\Skins folder.

13.5 About the Coveo SystemStatus Tool

The Coveo support team often needs detailed information on the state of your Coveo Enterprise Search (CES) server to be able to efficiently troubleshoot complex issues. The SystemStatus tool is available to easily gather a complete set of files describing the current state of your Coveo environment. You can use the tool to help you gather user dumps of the Coveo processes, a complete system status, or both.

13.5.1 Coveo SystemStatus Tool Requirements

Your environment must meet the following requirements to be able to use the Coveo SystemStatus tool:
Run the SystemStatus tool with administrator permissions

The Coveo SystemStatus tool gathers files from all over your Coveo environment. The user who runs the tool needs to have administrator permissions on your Coveo Master server and, if any, on all other Coveo Back-End servers (Mirror, Converter).

UAC considerations

When UAC (User Account Control) is activated on your Coveo server(s):

- With a one server Coveo environment:
  Run the SystemStatus tool in a command prompt with elevated rights.

- With a Master and Mirror server Coveo environment:
  Deactivate UAC on your all your Coveo Back-End servers before running the SystemStatus tool to ensure it is able to run correctly.

What’s Next?

Review the list of gathered files (see "Files Gathered by the Coveo SystemStatus Tool" on page 130).

13.5.2 Files Gathered by the Coveo SystemStatus Tool

The Coveo SystemStatus tool can gather two sets of files (System status and User dumps) listed below.

System status

The SystemStatus gathers the following files that are available when the SystemStatus tool runs:

- Export of registry key HKLM\SOFTWARE\Coveo\Enterprise Search\7
- File list for the CES installation folder
- File list for the CES CoreDumps folder
- File list for the CES index folders on all Coveo Back-End servers
- Copy of text files (*.txt) from the CES CoreDumps folder
- Copy of the mini dumps from the CES CoreDumps folder
- Copy of the SharePointInstaller*.Log files from the CES Bin folder
- Copy of the Coveo web.config file
- Copy of the CES index Config folder
- Copy of the PerformanceMng.txt file
- Copy of the mscordacwks.dll file
- Copy of the CES log files from the main index (last 15 days)
- Copy of the CES log files from the Slice and Mirror indexes (last 15 days)
- Copy of IIS and HTTPERR logs (last 15 days)
- Copy of the Windows Event Logs from all Coveo Back-End servers
- Copy of IIS Metabase configuration
- Index statistics
- List of the environment variables
- List of memory usage counters
- List of available disk space from all drives on all Coveo Back-End servers
- List of the processes that are running on the current server
- List of the versions of the DLLs in the Coveo Bin folder
- Output of the SystemInfo command on all Coveo Back-End servers
- Output of the netstat command for the server on which the SystemStatus tool runs

**User dumps**

The default user dumps option dumps any of the following processes that it finds running on the server:

- CESService(x).exe
- CESMirrorService(x).exe
- CESCrawler(x).exe
- CESConverter(x).exe
- CESExternalSecurityProvider(x).exe
- CESExchangeCallBackService.exe
- W3wp.exe

- File list for the CES index folders on all Coveo Back-End servers
- Output of the netstat command for the server on which the SystemStatus tool runs
- List of memory usage counters

**What's Next?**

Run the SystemStatus tool (see "Using the Coveo SystemStatus Tool" on page 131).

13.5.3 Using the Coveo SystemStatus Tool

The command prompt SystemStatus tool is easy to install and use.

13.5.3.1 Downloading and Installing

1. Using an administrator account, log on to your Coveo Master server.
download the latest version of the SystemStatus tool.

3. Extract the files to the root of a drive that you want to use.

**Example:** Extract to C:\SystemStatus.

13.5.3.2 Gathering System Information

1. Using an administrator account, log on to your Coveo Master server.

   **Notes:**
   - Ensure that the administrator account used meets the requirements (see "Coveo SystemStatus Tool Requirements" on page 129).
   - In a multiple Coveo server environment, ensure that UAC is deactivated on all Coveo Back-End servers before running the tool.

2. Start the SystemStatus tool:

   - When UAC is deactivated, simply double-click the [SystemStatus_Install_Path]\Coveo.Support.SystemStatus.exe file.

   OR

   - When UAC is activated in a single server Coveo environment:
     a. From the Windows **Start** menu, right-click **Command Prompt** and then select **Run As Administrator** to open a command prompt with elevated rights.
b. In the **Administrator: Command Prompt** window, change directory to the folder where you extracted the SystemStatus tool files, and then launch the `Coveo.Support.SystemStatus.exe` file.
3. In the command prompt window that appears:

   ![Command Prompt Window]

   a. The first time you run the SystemStatus tool, answer the following configuration prompts:

      i. At the **Automatically upload the results Yes/No** prompt, type **No**.

   b. Follow on-screen instructions to answer the following prompts for various options and storage path.
Following the last prompt, the gathering process starts. Depending on your selections, one or more other command line windows will open and the time required to complete the process may take several minutes.

**Important:** Do not close the main command prompt window. The time required to complete the process may take several minutes.

c. At the **Press Enter to exit** prompt, press Enter to close the main command prompt.

### 13.6 Getting Debug Information from a .NET Search Interface

You can add the `?&Debug=1` argument at the end of the .NET search interface address to list debug information.

**Example:** `http://localhost:8080/?&Debug=1`

The debug information appears at the bottom of the search results and contains **CES Settings**, **ASP.NET Settings**, **Search Settings**, and **User SID’s from server** sections.

```plaintext
Result Page 1

Debug Info

<table>
<thead>
<tr>
<th>CES Settings</th>
<th>ASP.NET Settings</th>
<th>Search Settings</th>
<th>User SID’s from server</th>
</tr>
</thead>
<tbody>
<tr>
<td>Server: localhost</td>
<td>Current User: NT AUTHORITY\NETWORK SERVICE</td>
<td>QuirksMode: False</td>
<td>Total #SIDs: 26</td>
</tr>
<tr>
<td>MirrorName: default</td>
<td>OS: Microsoft Windows NT 6.1.7601 Service Pack 1</td>
<td></td>
<td>everyone (S-1-1-0) (G-NT-0)</td>
</tr>
<tr>
<td>PhysicalIndexName: Default</td>
<td>nt authority\interactive (S-1-5-4) (G-NT-11)</td>
<td></td>
<td>local (S-1-2-0) (G-NT-141)</td>
</tr>
<tr>
<td>Impersonate: False</td>
<td>nt authority\authenticated users (S-1-5-11) (G-NT-6)</td>
<td></td>
<td>nt authority\remote interactive logon (S-1-5-14) (G-NT-143)</td>
</tr>
<tr>
<td>AllowAnonymousUsers: True</td>
<td>nt authority\this organization (S-1-5-15) (G-NT-139)</td>
<td></td>
<td>mandatory label=medium mandatory level (S-1-1-6-8192) (G-NT-157)</td>
</tr>
</tbody>
</table>
```

**Note:** The debug information feature can be disabled for all .NET search interfaces querying a CES instance. When disabled, adding `debug=1` to the URL has no effect. No message indicates the feature is disabled. A Coveo administrator can enable/disable the feature from the Administration Tool (see **Modifying Advanced CES Parameters**).

### 13.7 Gathering Windows Server Performance Monitor Information

You can use the Windows Server **Performance Monitor** to gather system performance information that can help the Coveo Support to troubleshoot Coveo server performance issues.
The following procedures describe how to configure the Performance Monitor to log processor, disk, and memory performance information, respectively for Windows Server 2008.

Enabling performance counter for processor, disk, and memory objects (Windows Server 2008)

1. Using an administrator account, connect to the Coveo server.
3. In the Run dialog box, type perfmon, and then click OK.
4. In Performance Monitor:
   a. In the panel on the left, expand Data Collector Sets.
   b. Right-click User Defined, and then select New > Data Collector Set in the contextual menu.
   c. In the first Create new Data Collector Set wizard dialog box:
      i. In the Name box, type CoveoPerformances.
      ii. Select Create manually (Advanced).
      iii. Click Next.
   d. In the second Create new Data Collector Set wizard dialog box:
      i. Select Create data logs.
      ii. Select the Performance counter check box.
      iii. Click Next.
   e. In the third Create new Data Collector Set wizard dialog box:
      i. Click Add.
         A. In the dialog box that appears, in the Available counters list, successively select the following performance counters, clicking Add for each of them:
            • Memory
            • PhysicalDisk
            • Processor
         B. Click OK.
ii. Click Finish.

f. When you are ready to start gathering performance information, in the main panel on the right, right-click **CoveoPerformances**, and then select **Start** in the contextual menu.

g. When you are ready to stop gathering performance information, in the main panel on the right, right-click **CoveoPerformances**, and then select **Stop** in the contextual menu.

5. To review the logged performance information, in Windows Explorer, locate and double-click the .blg file indicated in the **Output** column in the **Performance Monitor**.

The **Performance Monitor** opens showing the collected data.

6. Send the .blg file to the **Coveo Support**.
13.8 Using Transaction Trace Logging

You can enable trace logging for transactions to temporarily gather information that can help to identify exactly the transactions that are causing problems.

To use transaction trace logging

1. Go to the C:\tmp\ folder on the server that has the problem. Create the folder if it does not already exist.

   **Note:** The folder must be C:\tmp\, not C:\temp\, D:\tmp\ or any other variant.

2. In the folder, create a KIETransactionProfiling.flag empty file.

3. Switch the index to read-only mode and then back to read-write mode (see "Toggling the Index Between the Read-Write and Read-Only Modes" on page 263).

4. Let the system run for at least a day.

   A [Index_Path]\Index\Default\Default\Profiling\CESProfiling-Trn*.txt file is created for each slice.

   **Note:** The [Index_Path]\Index\Default\Default\Profiling\ folder must exist otherwise the log files are not created.

5. Disable transaction trace logging:

   a. Rename or delete the C:\tmp\KIETransactionProfiling.flag file.

   b. Switch the index to read-only mode and then back to read-write mode (see "Toggling the Index Between the Read-Write and Read-Only Modes" on page 263).

13.9 Using Query Profiling

A Coveo search interface typically returns results in less than one second. When you experience slower query performances, you can temporarily enable query profiling to gather information that can help identify the cause of the problem.

**Note:** CES 7.0.6196+ (November 2013) Query profiling files older than a month are automatically deleted.

To use query profiling

1. On the various Coveo servers (master, mirrors, slices, etc.) whose queries need profiling, go to the appropriate C:\tmp\ folder. Create the folder if it does not already exist.

   **Note:** The folder must be C:\tmp\, not C:\temp\, D:\tmp\ or any other variation.

2. In all C:\tmp\ folders where queries need profiling, create an empty KIEQueryProfiling.flag file.

3. Flags become effective (profiling activated) only once the next transaction is committed, which, by default, can take up to 5 minutes. You can make the flag effective immediately by manually forcing a commit (see "Forcing the Commit of a Transaction" on page 260).
4. Once the flag is effective, ensure that query performance issues occur:
   - If performance issues occur only from time to time, let query profiling run for a few days.
   - If performance issues can easily be reproduced, perform 10 to 15 slow queries.

5. Once query profiling files are acquired, turn off query profiling, in the C:\tmp\ folders, by renaming or deleting all relevant KIEQueryProfiling.flag files.

   **Note:** It is recommended to turn off query profiling as soon as possible to minimize the impact on server resources, particularly when the rate of queries is high.

6. Gather the master server configuration and all relevant query profiling files for each mirror and slice for the appropriate dates:
   - [Index_Path]\Index\[Mirror_Name]\Profiling\CESProfiling-MirrorQuery_yyyy_mm-dd.txt
   - [Index_Path]\Index\[Mirror_Name]\[Slice_Name]\Profiling\CESProfiling-SliceQuery_yyyy_mm-dd.txt
   - [Index_Path]\Index\[Mirror_Name]\[Slice_Name]\Profiling\CESProfiling-SliceNestedQueries_yyy-mm-dd.txt

   **Notes:**
   - **CES 7.0.5989—(October 2013)** Profiling subfolders did not exist. Query profiling files were saved directly in the mirror and slice folders.
   - The name for both the default mirror and the default slice is Default, so a typical query profiling file path is:
     D:\CES7\Index\Default\Default\Profiling\n
7. Send the gathered configuration and query profiling files to Coveo Support to get assistance in identifying the cause and solution to your query performance issue.

13.10 Logging Information With log4net

Coveo Enterprise Search (CES) modules such as connectors take advantage of the Apache log4net library to allow you to gather detailed information about the process. Logging such information may be very useful while troubleshooting CES issues.

The typical scenario to use log4net is when you open a case with Coveo Support to resolve an issue and more process troubleshooting information is needed. The Coveo support agent sends you or recommends a sample log4net configuration file to use to gather the required information.

13.10.1 How log4net Works

When a CES module supporting log4net runs and an XML file with the .log4net extension and the same full name as the module executable exists, the module gets the log4net configuration from this file, and then outputs corresponding information.

The log4net configuration file does not have to exist when you start your CES. Log4net watches for any new file created in the folder so simply creating the .log4net configuration file triggers the update within the component.
that is logging. When using a file appender, the destination folder does not have to exist. Log4net creates the folder.

To log information with log4net

1. Using an administrator account, connect to the Coveo Master server.

2. Using a text editor:
   
a. Open the log4net configuration file that you received from Coveo Support or a sample log4net configuration file appropriate for the CES module for which you want to log information.

   **Note:** CES 7.0.7104+ (October 2014) The following sample log4net configuration files are available from the [CES_Path]\bin\Log4Net Samples\ folder:

   - CESCustomCrawlers7.exe.log4net
     To log information from connector (crawler) processes.

   - Coveo.CNL.HostProcess.exe.log4net
     To log information from the child processes launched by some connectors such as the Database connector.

     To log information from the security provider processes.

   b. In the file, edit the lines that typically need to be customized:
Example: The following is a typical content of a sample log4net configuration file for a connector.

```
<log4net>
  <!-- RollingFileAppender - Use for long lasting logging sessions -->
  <!-- NOTE : DO NOT FORGET TO CHANGE THE LOG PATH -->
  <!-- NOTE : If you think that a lot of logs will be generated, change the
  maxSizeRollBackups value -->
  <appender name="RollingFileAppender" type="log4net.Appender.RollingFileAppender">
    <file value="C:\Temp\Crawler.logs" />
    <appendToFile value="true" />
    <rollingStyle value="Size" />
    <maxSizeRollBackups value="10" />
    <maximumFileSize value="50MB" />
    <staticLogFileName value="true" />
    <lockingModel type="log4net.Appender.FileAppender+MinimalLock" />
    <layout type="log4net.Layout.PatternLayout">
      <conversionPattern value="%date [%thread] %-5level %logger - %message%newline" />
    </layout>
  </appender>
  <!-- Example logger -->
  <!-- NOTE : To activate a logger, you need to specify the name and uncomment the
  following lines -->
  <!--
  <logger name="Coveo.CES.CustomCrawlers.MyCrawler">
    <level value="DEBUG" />
    <appender-ref ref="RollingFileAppender" />
  </logger>
  -->
</log4net>
```

- In the `appender` section, ensure that the output file value points to an appropriate drive, folder, and file name.

  **Example:** When want to log crawling information in the `C:\Temp\` folder:

  ```
  <file value="C:\Temp\Crawler.logs" />
  ```

- In the `logger` section, ensure that the name attribute contains the appropriate namespace. Contact Coveo Support for assistance when you do not know the namespace.

  **Example:** When you want to see what happens with the connection to Google Drive for a source, you can use the CESCustomCrawlers7.exe.log4net sample file with the following `logger` section:

  ```
  <logger name="Coveo.Connectors.GoogleDrive.Connection">
    <level value="DEBUG" />
    <appender-ref ref="RollingFileAppender" />
  </logger>
  ```

- When the `logger` section is commented, remove the commenting markers `<!-- -->` around it to activate the logging.

  **Note:** For more information on the syntax of the log4net configuration file, refer to the Apache log4net documentation, or contact Coveo Support.

c. Save the file in the `[CES_Path]\bin\` folder.

3. Ensure that the CES module for which you are collecting logs performs the actions you want to log.

4. Open the log file to review the logs.
5. Once you got the information that you want, deactivate the logging using one of the following methods:
   - Rename the log4net configuration file.
     
     **Example:** You can add the .DISABLED extension to the file to indicate its state.
     
     `[CES_Path]\bin\CESCustomCrawlers7.exe.log4net.DISABLED`
     
     When you want to restart logging similar information, you only need to remove the .DISABLED extension.
     
     OR
   
   - Move the log4net configuration file to another folder such as `[CES_Path]\bin\Log4Net Samples\`.
     
     OR
   
   - Delete the log4net configuration file.
     
     OR
   
   - Using a text editor open the log4net configuration file in the `[CES_Path]\bin\` folder, and comment all the logger sections by adding commenting markers `<!- -!>` around them, and then save the file.

   **Important:** It is not recommended to leave active log4net logging for long periods as this process can slow down the CES module that is outputting the logs.

13.11 Why Are Some Documents Not Returned by the Search Engine?

If a document containing all the terms queried (including field data and exact phrases) is not displayed in the search results, it is possible that it has not been indexed or—for recently added sources—that the transaction has not been written yet. The following table lists possible problems, as well as their solutions.

**Note:** The Index page (Logs > Index) provides detailed information about recent indexing operations—including the name and path of rejected documents (see "What Information Is Displayed in the Index Log?" on page 398).

<table>
<thead>
<tr>
<th>Problems</th>
<th>Solutions</th>
</tr>
</thead>
<tbody>
<tr>
<td>The transaction is not committed.</td>
<td>Force-commit the transaction:</td>
</tr>
<tr>
<td></td>
<td>In the Index Content section of the Overview page (Status &gt; Overview), click Commit Current Transaction.</td>
</tr>
<tr>
<td>Problems</td>
<td>Solutions</td>
</tr>
<tr>
<td>----------</td>
<td>-----------</td>
</tr>
</tbody>
</table>
| Subfolders or subsites are not indexed. | Index subfolders or subsites, and rebuild the source:  
1. On the Coveo server, access the Administration Tool.  
2. Access the Sources and Collections page (Index > Sources and Collections).  
3. In the Sources section, expand the source drop-down list.  
4. Select Edit General Properties. The General page corresponding to the source is displayed.  
5. In the Options section, select Index subfolders.  
6. Click Apply Changes.  
7. Click Rebuild. |
| The content of SharePoint sites is not indexed. | Index SharePoint sites and rebuild the source:  
1. Access the Sources and Collections page (Index > Sources and Collections).  
2. In the Sources section, expand the SharePoint source drop-down list.  
3. Select Edit General Properties. The General page corresponding to the source is displayed.  
4. In the SharePoint Sites to Index section, select Index only the sites listed in the Portal SiteDirectory or Index all sites (CES must be integrated to SharePoint).  
5. Click Apply Changes.  
6. Click Rebuild. |
| The content of SharePoint personal sites is not indexed. | Index SharePoint personal sites and rebuild the source:  
1. Access the Sources and Collections page (Index > Sources and Collections).  
2. In the Sources section, expand the SharePoint source drop-down list.  
3. Select Edit General Properties. The General page corresponding to the source is displayed.  
4. In the Options section, select Index personal sites.  
5. Click Apply Changes.  
6. Click Rebuild. |
| The document is subject to an exclusion filter. | Remove or modify the exclusion filter:  
1. Access the Sources and Collections page (Index > Sources and Collections).  
2. In the Sources section, expand the source drop-down list.  
3. Select Edit Filters. The Filters page corresponding to the source is displayed.  
4. Delete or modify the exclusion filter to include the document.  
5. Click Rebuild. |
<table>
<thead>
<tr>
<th>Problems</th>
<th>Solutions</th>
</tr>
</thead>
<tbody>
<tr>
<td>The action for the document type is <strong>Reject document</strong> or <strong>Index file information only</strong>.</td>
<td>Select the <strong>Index entire document</strong> action for the document type and rebuild the source:   1. Access the <strong>Sources and Collections</strong> page (<strong>Index &gt; Sources and Collections</strong>).  2. In the <strong>Sources</strong> section, expand the source drop-down list.  3. Select <strong>Edit Document Types</strong>. The <strong>Document Types</strong> page corresponding to the source is displayed.  4. Click <strong>Edit</strong>. The document type set used with this source is displayed.  5. Click the name of the document type to edit. The document type properties are displayed.  6. In the <strong>Action</strong> drop-down list, select <strong>Index entire document</strong>.  7. Click <strong>Apply Changes</strong>.  8. Click <strong>Rebuild</strong>.</td>
</tr>
<tr>
<td>The document is of a type not supported by CES converters.</td>
<td>Use an IFilter to convert the document in a format recognized by CES and rebuild the source:  1. From a third-party source, download the appropriate IFilter for the document type.  2. Access the <strong>Sources and Collections</strong> page (<strong>Index &gt; Sources and Collections</strong>).  3. In the <strong>Sources</strong> section, expand the source drop-down list.  4. Select <strong>Edit Document Types</strong>. The <strong>Document Types</strong> page corresponding to the source is displayed.  5. Click <strong>Edit</strong>. The document type set used with this source is displayed.  6. Click <strong>Load IFilter Mapping</strong>. Document types are automatically associated with corresponding IFilters on the server.  7. Access the <strong>Sources and Collections</strong> page (<strong>Index &gt; Sources and Collections</strong>).  8. In the <strong>Sources</strong> section, select the sources to rebuild.  9. In the <strong>More Actions</strong> drop-down list of the <strong>Sources</strong> section, select <strong>Rebuild</strong>. The selected sources are rebuilt.</td>
</tr>
<tr>
<td>The document is written in a language not recognized by CES and the option selected for <strong>Language Detection</strong> is <strong>Reject the document</strong>.</td>
<td>Modify the <strong>Language Detection</strong> option to index documents even if their language is not recognized and rebuild the source:  1. Access the <strong>Converter Managers</strong> page (<strong>Configuration &gt; Converters</strong>).  2. In the navigation panel on the left, click <strong>Languages</strong>. The <strong>Languages</strong> page is displayed.  3. In the <strong>Language Detection</strong> section, select <strong>Index</strong>.  4. Click <strong>Apply Changes</strong>.  5. Access the <strong>Sources and Collections</strong> page (<strong>Index &gt; Sources and Collections</strong>).  6. In the <strong>Sources</strong> section, select the sources to rebuild.  7. In the <strong>More Actions</strong> drop-down list of the <strong>Sources</strong> section, select <strong>Rebuild</strong>. The selected sources are rebuilt.</td>
</tr>
</tbody>
</table>
The CES service authentication does not have sufficient permissions to open the document. (Applies to local/network, Exchange, SharePoint and Lotus Notes sources).

Modify the CES logon account and rebuild collections containing local/network, Exchange, SharePoint and Lotus Notes sources.

**Note:** If the collections contain thousands of documents, rebuilding them can be long. Because they cannot be queried while they are being rebuilt, it is suggested to rebuild them outside of business hours.

1. Access the Windows Control Panel (Windows Start menu > Control Panel).
2. Double-click Administrative Tool.
3. Double-click Services. The Services window is displayed.
4. In the Services (Local) section, double-click Coveo Enterprise Search 7. The Coveo Enterprise Search 7 Properties (Local Computer) dialog box is displayed.
5. Click the Log On tab.
6. In the Log on as section, select This account and enter an account name and password with sufficient permissions to open restricted documents.
7. Click Apply.
8. In the Administration Tool, access the Sources and Collections page (Index > Sources and Collections).
9. In the Collections section, select the collections to rebuild.
10. In the More Actions drop-down list of the Collection section, select Rebuild. The selected collections are rebuilt.

13.12 Why does the Initial .NET Search Page Take Much Longer to Appear?

You might sometimes find that the loading of the initial Coveo .NET search interface page takes significantly longer than the following ones. The Coveo .NET search page is an ASP.NET application. An ASP.NET application takes a non-negligible time to load in the web server (IIS). Once loaded, subsequent requests to the application are returned much faster by IIS.
By default, ASP.NET Web pages are compiled dynamically when users first request a resource from a web site. After pages have been compiled the first time, the compiled resources are cached, so that subsequent requests to the same page are significantly more efficient. By default, IIS closes applications that have been inactive for some time. The next user requesting service from that closed application will experience a slow response while waiting for the initial loading to complete.

You can solve this problem by configuring CES to periodically send requests to a search application to ensure it is continuously loaded in IIS.

**Note:** Refer to the Understanding ASP.NET Dynamic Compilation MSDN document for more information.

### 13.13 Cannot Connect to the Instance Default

The **Error** dialog box with the **Cannot connect to the instance default of Coveo Enterprise Search hosted on...** message may appear when you try to open one of the CES user interfaces (Administrator Tool, Interface Editor, Console).

One or more of the following conditions may be the cause of this error:

- The log on account that the CES service uses has changed.
  
  The password or the username that was specified for the CES service when CES was installed may have changed. When the password of this account changes in Active Directory, you must also manually change the log on information for the CES service on the Coveo server (see "Modifying the CES Log On Account" on page 227).

  **Note:** A best practice is to create a user account dedicated to the CES service with a password that does not change, or does not change frequently (see "About the CES Service Logon Account" on page 225).

- The account with which you logged in to the Coveo server does not have administrator rights.

  Log on to the Coveo server with an account that has administrative rights and try again.

- The CES service is not started.

  The CES service does not start when either of the previous conditions occur. Ensure to fix them when needed, and then start the CES service (see "Starting the CES Service" on page 248).
13.14 Access Denied Message When Opening a Result

An **Access Denied** message may appear in the search interface when:

- A user clicks a search result title to open it.
- The account used to query the index has insufficient permissions to access the document.

This problem occurs only when source permissions override file permissions.

To fix this problem, consider the following solutions for the source with which this problem occurs:

- Change the source permissions (see "Modifying Source Security Permissions" on page 297).
- Configure CES to display the Quick View instead of the actual document. You need to select the **Generate a cached HTML version of indexed documents** and **Open results with cached version** options for this source (see "Modifying General Source Parameters" on page 292).

13.15 Certificate Error

The Coveo Platform 7 uses search security certificate to manage connections between Coveo Front-End and Back-End servers. When an element of the certificate security configuration is missing, you can get error messages such as the following:

```
FailedToImpersonateUsersException: There was no certificate provided by the client while trying to impersonate users. Either provide a trusted client certificate with impersonation rights or login with requested credentials.
```

Validate that all the elements of the certificate security configuration are in place in your Coveo deployment (see "About Search Security Certificate" on page 235).

13.16 Cannot Find SharePoint Documents

**Symptoms**

After configuring and building or refreshing a SharePoint source, you cannot find the SharePoint documents in the search interface.

In the CES logs, a message similar to the following one appears when the source and the security cache are refreshed:

```
Error while expanding group <Member name="Web Application Policy - Full Control" type="Group"><Info key="CrossSite" val="true"/>\<Info key="SiteURL" val="https://[Coveo_Server]/[User_Path]/"/>\</Member> (class CGLSharePoint::RemoteCallFailedException: Server was unable to process request. ---) Attempted to perform an unauthorized operation.)
```

**Possible cause**

The user identity needed by the SharePoint Security Provider to crawl the SharePoint source is missing. When
this is the case, the Security Provider cannot expand users and therefore cannot determine who can access SharePoint documents, so nobody can find the SharePoint documents in the search interface.

Solution

Assign an appropriate user identity to the Security Provider associated with the SharePoint source.

13.17 Resolving Slow Search Interface Loading in Sitecore

When a Coveo .NET Front-End search interface is integrated in a Sitecore website (see "Integrating the Coveo .NET Search Interface in a Sitecore Website" on page 158), long search interface page loading time can be experienced.

Note: This topic is not applicable to Coveo for Sitecore, but rather to a legacy integration of a Coveo .NET Front-End search interface in Sitecore.

This unusual slow rendering of the Coveo search interface pages may be caused by the Sitecore cache settings. The Coveo search interfaces take advantage of browser caching to prevent repeatedly loading frequently used components, and therefore significantly reduce page loading time.

To resolve slow search interface loading in Sitecore

1. Using an administrator account, connect to the Sitecore server.

2. Using a text editor:
   a. Open the Sitecore web.config file.
   b. In the file, as shown in the following web.config file excerpt, ensure that DisableBrowserCaching is set to false.

   ```xml
   <!-- DISABLE BROWSER CACHING
   If true, all pages will have:
   Cache-Control: no-cache, no-store
   Pragma: no-cache
   in the http header
   -->
   <setting name="DisableBrowserCaching" value="false" />
   ```
   c. Save the file.

13.18 Security Provider Not Properly Configured

Symptom

You may notice in the Administration Tool Overview page that either of the following error message appears in the System State section:

- A security provider is not properly configured.
- Some security providers are not properly configured.
Open the CES Console to locate and review the error messages that indicate which security provider has a problem and what is the cause of the problem (see "Using the CES Console" on page 246).

Possible causes and solutions

- Repository is not warmed up and the security provider failed to initialize

  When a security provider starts, it needs to access the specified repository to complete its initialization. When the repository takes too much time to respond, the security provider connection attempt times out.

  **Example:** When your Sitecore security provider starts following an over-night CES maintenance restart, your Sitecore server is not used much at this hour and IIS needs to reload the site to respond to the security provider requests. The security provider reaches the connection timeout. In the CES Console you see a message of the form:

  ```
  The security provider "[SecurityProviderName]" could not be contacted for registration: CGKNetwork::PacketChannel::CannotOpenChannelException: The system cannot find the file specified.
  ```

  1. Ensure that the repository is warmed up.

  2. In the Administration Tool, access the configuration page for the security provider that has the problem ([Configuration > Security Providers]).

  3. Click **Apply Changes** to launch a new initialization attempt.

  4. In the CES Console, review the security provider messages to ensure that it starts without errors.

- Missing security provider parameter
**Example:** In the CES Console, you see a message of the form:

An error occurred while initializing the Blade "[SecurityProviderName]" (ID # [n]): Error: The Security Provider "ServerBaseAddress" parameter is missing.

Review the configuration of the security provider to add the missing parameter with the appropriate value (see "Adding or Modifying a Security Provider" on page 417).

- **Bad configuration value**

**Example:** In the CES Console, you see a message of the form:

An error occurred while initializing the Blade "[SecurityProviderName]" (ID # [n]): Unable to connect to this address: 'http://YourRepositoryServer/'

Review the configuration of the security provider to set a valid address for the server of your repository. If the address is correct, validate that the server is available (see "Adding or Modifying a Security Provider" on page 417).

**Example:** The password for the Windows user referenced in the user identity assigned to a security provider changed in Active Directory but not in CES. In the CES Console, you see a message of the form:

An error occurred while initializing the Blade "[SecurityProviderName]" (ID # [n]): Unexpected exception in method 'InitBlade': CoveoConnectors.Sitecore2.Exceptions.Sitecore2WebServiceException'1 [System.Exception]: Invalid username or password.

Review the configuration of the security provider to ensure that the username and password of the assigned user identity are still valid (see "Adding a User Identity" on page 420).

### 13.19 Time Zone Error

The Coveo search interface presents date/time values adjusted to the time zone of the computer with which you access the search interface. When the computer accessing the search interface and the Coveo Front-End server are in different time zones, like when an end-user is traveling, in the search interface, the end-user may see a warning message similar to the following one:

The time zone string reported by your computer (Tokyo Standard Time) is invalid. The results are displayed for the local time zone of the Coveo Master server (Eastern Standard Time).

**Possible causes**

- On the Coveo Front-End server, the time zone from which the end-user is accessing the search interface may not be defined in the Windows registry.

- On the end-user computer, the time-zone value can be missing, in an incompatible format, or corrupted.

- A network device or process such as a proxy between the client and the server can intercept and modify the query received by the Coveo server.

**Possible solutions**
- On the Coveo Front-End server, fix the time zone registry keys (see Missing time zones - Microsoft Community).
- On the end-user computer, verify the time zone in the operating system parameters.

13.20 Unsupported Back-End Version for a .NET Search Interface

The Coveo .NET Front-End validates the compatibility of the Coveo Enterprise Search (CES) version to which it connects on the Coveo Master server (Back-End). When the versions of Coveo .NET Front-End and Coveo Enterprise Search are not compatible, you will see an error message similar to the following one:

The CES version for the specified server is not compatible with the Coveo .NET Front-End version that you are configuring. CES version X.X.XXXX or higher is required.

Possible causes
- You upgraded Coveo .NET Front-End and your Coveo Enterprise Search does not support new Front-End features.
- You installed a new Coveo .NET Front-End version and bypassed the installation warning notifying you that your Coveo Enterprise Search was too old. Your Back-End does not support new Front-End features.

Possible solution
- On your Coveo Master server, upgrade your Coveo Enterprise Search (see "Upgrading CES" on page 79).

13.21 SharePoint Error - Number of Lookup Columns

Symptom

When your indexed SharePoint content contains tables with several lookup columns, you can get an error message similar to the following when you rebuild your SharePoint source:

A SharePoint error was encountered while refreshing (Cannot load the items for the list "[List_Name]" of the SharePoint site "[Site_Name]". Reason: class CGLSharePoint::RemoteCallFailedException: The query cannot be completed because the number of lookup columns it contains exceeds the lookup column threshold enforced by the administrator.0x80070093)

Possible Cause

The SharePoint content contains documents with lookup (and workflowstatus) fields exceeding the limit set by the SharePoint List View Lookup Threshold parameter, by default 8.

Possible Solutions
- Increase the value of the SharePoint List View Lookup Threshold parameter (see SharePoint 2010/2013: List view Lookup threshold uncovered).
- Reduce the number of lookup (and workflowstatus) fields in your SharePoint document.
13.22 About the Unused Parameter Warning Message in the CES Console

A warning message appears in the CES Console (see "Using the CES Console" on page 246) when you build a source and one of the configured hidden parameter has an invalid name. The message looks like the following:

Parameter 'X' was configured on the source 'Y' but was not used by the connector. Consider removing it or fixing its name.

Possible cause

You add an hidden parameter in a source configuration page and make a typo in its name.

Example: You want to add the DiscoveryServiceUrl hidden parameter, but make a typo (DiscoveyServiceUrl) when configuring a Microsoft CRM Dynamics source (see "Modifying Hidden Microsoft Dynamics CRM Source Parameters" on page 1171).

Possible solution

Correct the parameter's name or remove it, and then rebuild the source.