datto | FILE BACKUP & SYNC

Datto Workplace

Security Architecture Guide

Table of Contents

Operational Security

Dedicated Geo-Redundant Data Center Infrastructure

As opposed to the common virtualized approach to cloud services, in which cloud service providers lease processing and storage capacity from Internet infrastructure providers, **all Datto Workplace hardware and software in each data center is 100% owned, operated, and managed by Datto**. In typical virtualized cloud environments, service applications and customer data actually share processing and storage platforms in a virtual time-sliced manner, resulting in a minimum of separation between independent operating domains. The dedicated data center approach in which Datto has invested ensures that only Workplace services operate on Workplace hardware or software processing and storage platforms.

True 100% isolation of the Workplace service eliminates the possibility of experiencing service interruption, performance degradation, or malware infection that might otherwise be caused by adjacent applications. Combined with multi-level regional and data center redundancy, the Workplace infrastructure represents one of the most secure, reliable, and available cloud service architectures available today.

Workplace uses a co-location model for deployment of Datto-owned and -operated equipment and software, utilizing the rack space, power, cooling, and physical security of major world-class SSAE 16 audited data centers. These facilities are classified as Tier 3 or better with N+1 fault tolerant systems guaranteeing 99.982% availability. The Workplace network architecture deployed to these facilities includes multiple levels of redundant application servers and storage arrays, ensuring high availability, failover support, and load balancing.

Datto operates data centers in several different geographical regions, including the United States, Canada, Denmark, and Australia, and is planning further expansion into other regions. Within each region, there are two levels of redundancy. First, within each data center, redundant servers and file storage ensure that data center-level failures can be isolated and resolved quickly. Second, within each region, at least two independent data centers are physically distanced and isolated from each other, thus providing protection from higher level data center failures, regional disasters, and broader Internet-related failures. This dual-level geo-redundancy provides the greatest possible availability and protection against data loss.

The physical presence of data centers in separate regions also means that data does not leave the region. Data stays in the United States for U.S. customers, in the European Union for EU customers, in Australia for AU customers, and in Canada for Canadian customers (in compliance with PIPEDA and local regulations).

The General Data Protection Regulation (GDPR), which fundamentally changed European privacy law, went into effect in May 2018. It requires all companies that handle the "personal data" of individuals in the EU to adopt more stringent privacy and security practices. Datto has made a substantial investment of time and resources to ensure its products and services are GDPR compliant.

Summary

- Co-location model with HW and SW 100% owned, operated, and managed by Datto
- Geo-redundant, Tier 3, SSAE16 Audited data centers (two per region)
- Complete, redundant, regional data set in each data center
- Complete regional server setups in each data center
- Data center redundancy using RAID6 mirrored backup with replication
- Modular clustered server farms for service load-balancing and failover protection
- SLAs for response time, service restoration, and 99.982% availability

SSAE 16 / SAS 70 and SOC2 Audits

In the rapidly changing landscape of cloud services, companies that handle sensitive information in, for example, the legal, finance, and medical sectors find that their information processing controls are under increasing levels of scrutiny. **Workplace data centers are audited against both AICPA SSAE 16/SAS 70 and ISAE 3402 criteria for system availability and security,** thus providing assurances regarding adequate information processing controls oversight. Similarly, Workplace's own internal security controls are audited against SSAE 16/ISAE 3402 criteria for employee policies, physical and logical access controls, intrusion detection and testing, service reporting, security incident procedures, training, change control, and configuration management.

Workplace's SOC2 Type 2 examination report is issued in accordance with both the SSAE 16 attestation standards established both the American Institute of Certified Public Accountants and the attestation standards established by the International Standard on Assurance Engagements (ISAE) 3402, known as "Assurance Reports on Controls at a Service Organization." Accordingly, Workplace services can serve as a foundation upon which customers can build their SSAE 16/SAS 70/ISAE 3402 compliant data processing and storage policies and practices.

Logical Access Security

All Datto Workplace application servers are protected with OS security modules that apply Discretionary Access Control and Mandatory Access Control policies to all server processes, thus ensuring that no software process can be gainfully subverted.

All Workplace infrastructure connection pathways are highly regulated as to the types of traffic allowed between various internal server endpoints. Any network traffic that does not meet the expected data flow patterns in terms of source, destination, and/or traffic type is immediately interrupted and reported to monitoring personnel through alerts. All known attack vectors are explicitly prohibited.

All of the Workplace regional data centers are monitored 24 hours a day, 365 days a year

Comprehensive Monitoring

All Workplace regional data centers are monitored 24 hours a day, 365 days a year by equipment service and operations staff who have immediate access to Workplace engineering personnel in the event that it becomes necessary. Co-location with major world-class data center industry partners ensures that our physical and environmental security is unsurpassed.

Workplace utilizes dedicated software monitoring components that are designed to track and evaluate the operation of servers, networking equipment, applications, and services within the Workplace service infrastructure. This includes monitoring of resources such as processor load and memory and disk space usage.

Alerts regarding performance or potential security issues are automatically distributed to several on-call staff via SMS and email.

Testing, Risk Assessment and Compliance

Datto Workplace makes use of independent 3rd-party testing, analysis, and assessment services. Workplace's multi-faceted approach to testing and risk assessment incorporates ongoing 3rd party penetration testing of Web, Agent, and APIs, Periodic SAS/SSAE audits, and Daily Hacker Safe updates.

The General Data Protection Regulation (GDPR) became enforceable on 25 May, 2018. The GDPR replaces the Data Protection Directive 95/46/EC and helps to standardize legal data protections across the Member States of the European Union. Datto is aware of its obligations as a processor under the GDPR and remains committed to helping support its MSP Partners and their clients' GDPR compliance efforts.

Datto, Inc. has certified certain of our services, for which we act as a data processor, under the EU-U.S. Privacy Shield Framework. For more information on Privacy Shield, please visit the U.S. Department of Commerce's Privacy Shield website at: https://www.privacyshield.gov/welcome

Workplace is compliant with all Security Rules specified in the Technical Safeguards, Administrative Safeguards, and Physical Safeguards from the Health Insurance Portability and Accountability Act (HIPAA) of 1996. Workplace's Privacy Policy provides details regarding the policies implemented throughout Workplace in order to comply with HIPAA. Furthermore, Workplace engages health care provider customers as HIPAA Business Associates through BAA agreements.

Data Encryption and Authentication

All files handled by the Datto Workplace service are secured, both in transit and in storage, using 256-bit AES-encryption. In order to maximize the separation between teams, users, and files, a different unique rotating encryption key is used for each individual file. None of the encryption keys are stored "in the clear" in any non-volatile storage, but rather are encrypted and stored under the protection of a master key. Authentication is ensured through the use of certificate-based server authentication, which ensures that the user's agent will neither connect nor cooperate with any server other than those that comprise the Workplace service. Even in the unlikely event of a successful attack on Internet DNS or routing infrastructure, which is outside the control of Workplace or any other SaaS provider, Workplace's certificate-based authentication will ensure that no malicious agent could successfully connect to the Workplace service.

All files handled by the Datto Workplace service are secured, both in transit and in storage, using 256-bit AES-encryption.

Policy Profiles

Team Defaults and Policies provide Workplace administrators with **granular control of the features and functions available to users**. Given that policy profiles are cumulative, applying them to both groups and individuals offers the best possible balance between ease of administration and granular control. All policies referenced in this guide are controlled using this mechanism.

User Management and Policies

User Security Roles

Datto Workplace provides Role-Based Access Control (RBAC) mechanisms through which specific users can be granted varying levels of administrative permissions. Users can be granted Super Admin or Admin security roles, providing an extensive set of controls and management tools that ensures flexible, powerful, and effective administration of the team. These security roles allow administrative control of:

- Users and groups
- Default policies and policy profiles
- Active Directory (AD)
- Remote deployment
- Device approval
- Remote device wipe
- Reports

Authentication Policies

Datto Workplace user authentication (excluding authentication via Active Directory and SSO) can be managed with policies, allowing password requirements and Two-Factor Authentication to be enforced. Password requirement policies define a variety of values such as password expiration, reuse cycle, and recent password intervals, as well as password complexity and failed login thresholds for account lockout.

Datto Workplace supports the delivery of 2FA tokens through either SMS or through RFC-6238 compliant mobile apps, such as Google Authenticator, that utilize Time-based One-time Password Algorithm (TOTP) tokens..

Datto Workplace's 2FA feature also supports a **2FA IP Address Whitelist,** which allows administrators to specify one or more source IP address that can be exempted from 2FA authentication requirements. This feature is commonly used to "whitelist" corporate headquarters or other remote offices, where there is high confidence that login attempts are from valid users physically located on company property, behind company firewalls.

Active Directory Integration

User authentication and account management for users and groups can be enabled through the Active Directory (AD) integration. This feature allows Workplace administrators to provision users and groups using metadata from AD, and to require all AD-managed users to authenticate using their AD credentials. Workplace does not maintain any login information during user authentication, but acts as a proxy between the user and Active Directory servers.

Single Sign-On

Datto Workplace users can **benefit from the security and convenience of authenticating via a SSO IdP** (Identity Provider) to access the Workplace service. Datto Workplace uses the SAML 2.0 protocol to authenticate access to the Workplace service.

IP Address Whitelist Policies

The IP Address Whitelist is also commonly referred to as an Access Control List (ACL) in computer networking security terminology. This feature enables Workplace administrators to place a flexible set of restrictions on service login. Specifically, service login can be allowed or prohibited based on a combination of the mode of access (Workplace Online, Workplace Mobile, Workplace Desktop) and the source IP address. For example, this might be configured to allow access via web browsers and mobile devices from anywhere, while restricting Workplace Desktop access to your company offices' IP address range.

Session Policies

Session Policies allow Workplace administrators to **specify session timeout duration and prevent the remember-me feature** for added control of user sessions into Workplace services.

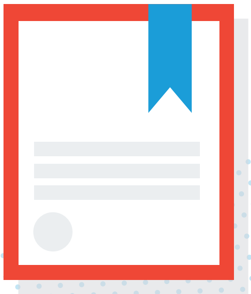
User authentication can be managed with policies, allowing password requirements and 2FA to be enforced.

Device Management and Policies

Cloud-based file sync and share services provide customers with significant advantages in terms of access mobility, ease of sharing, and real-time collaboration. This broadening access, however, means that virtual data boundaries of business organizations have expanded to include a greater variety of devices over a wider geographical area. Furthermore, this includes both business-owned and personal devices. Workplace mitigates the potential for increased security threats by providing a set of device management features which are integrated into Workplace Access Management.

Remote Wipe

Businesses have a critical need to ensure that all company data is securely and completely removed, on demand, from lost or stolen devices or from the devices of departing employees. The proliferation of mobile devices and the hybrid use of personal devices in business environments only serves to amplify this need. Consequently, **Workplace supports remote removal of company data from computers and mobile devices.**



Workplace supports remote removal of company data from computers and mobile devices.

Remote Wipe can be performed manually by administrators, on any device, or by users on their own devices. Administrators can also configure policies that trigger automatic remote wipe when a user is disabled or deleted in Active Directory, or after excessive login attempts on Workplace Mobile.

Workplace's Device Wipe capability is an "atomic" feature, and encompasses the entire wipe process, from initial manual request or automatic trigger to final confirmation. After a Device Wipe is initiated for a target device, the Workplace service monitors for a connection from that device. Upon connection, the Workplace service quarantines the connection while commanding the remote device to wipe all Workplace-synced files from the device. After the wipe is completed, the device status is flagged with a positive confirmation so that administrative personnel are certain that the operation was successful.

Remote Device Management

Datto Workplace allows administrators to lock Workplace Desktop preferences, thereby preventing users from changing settings. This, used in conjunction with other Workplace Desktop policies, provides complete remote management, including:

- Location of the Workplace folder
- Projects synced to the device
- Maximum bandwidth usage
- The ability to remotely access the device on which Workplace Desktop is installed

Mobile Device Management

Workplace Mobile begins with a strong foundation of security, using local encryption of all data stored by Datto Workplace Mobile. **Workplace also uses Device Pinning techniques to ensure that the "approved" mobile device/app is permanently associated with the approved user account.** These techniques are critical to the control of both company data and user activities.

Mobile device policies allow administrators to set policies regarding the functionality available via the mobile app. The following policy settings are available:

- **Enforce Authentication** - Specifies whether authentication is required to access accounts via Workplace Mobile. Also controls the authentication security level.
- **Enable/Disable Sync** - Controls the ability of users to sync files to their mobile device
- **Account Validation** - Specifies the number of days a user can remain offline and still access content via the Workplace Mobile app. After the predefined period, access will be denied until the user connects to the Internet. This mitigates the risk of a user putting a device into Airplane Mode and accessing company data indefinitely.
- **Enable/Disable Content Adding & Creating** - Controls the ability of users to add or create content on their mobile device and upload it to Workplace
- **Enable/Disable Editing** - Controls the ability of users to edit company files that have been downloaded or synchronized to the mobile device
- **Enable/Disable Exporting (Open-In 3rd Party Apps)** - Controls the ability of users to export company files to third party apps installed on their mobile device

Data Management and Security

Workplace's security architecture provides content access control on two levels. First, overarching user policies are established by administrators and enforced by the Workplace service. Then, within the confines of those policies, users are free to grant others access to the content they control at whatever level they feel is appropriate.

Content owners can also delegate the ability to share the content with other users and to create public shares.

Team Shares

Access permissions to projects or sub-folders can be set to Online View Only, Read-Only, Modify, Create & Modify, and Full Access (including delete). In addition, **content owners can also delegate the ability to share the content with other users and to create public shares.**

Public Shares

If permitted via policy, and if granted permission from the content owner, Datto Workplace users can establish and manage public shares to projects, folders and files. Public shares can be password protected and/or configured with expiration criteria. The functionality available to public share recipients can be configured as follows:

- View Only (via a web browser)
- View and Download
- Direct Download (files only)
- Upload Only (projects and folders only)
- View and Upload
- View, Download, and Upload
- Edit, Download, and Upload (allows document editing via Microsoft Office 365)

File Locking, File Versioning and Conflict Management

Additional protection of content includes several cooperating mechanisms that defend against accidental deletion or overwriting of files. While the file lock mechanism alerts other users during the collaborative editing of documents, the file versioning and file branching mechanisms operate automatically to ensure that, even in the event of file conflicts or file overwrite, no content is lost.

Users can manually lock files to prevent other users from making changes. In addition, Microsoft Office files automatically lock when edited, and automatically unlock once closed. Workplace Server converts local application locks on the file server into a Workplace lock, and vice-versa, providing improved collaboration between on-premises and remote users.

As users edit and save subsequent versions of a file, the **file versioning feature automatically retains the previous versions of all files for up to 180 days.** At any point during that period, users can access previous versions through the Workplace web portal.

File branching, a similar back-end automatic process, ensures that conflicting updates to files are retained. If users ignore a file lock or are, due to lack of Internet connectivity,unaware that another user has updated the file, the changes will be saved in a duplicate version appended with the user's name. This mechanism ensures that all changes are retained.

Datto Workplace has built-in, sophisticated Ransomware Detection and Recovery.

Full Control of Content

Workplace's Manage Projects feature facilitates full control of file structure and sharing permissions to ensure compliance with company guidelines. This feature allows Super Admins to...

- View and manage the entire team file structure
- Manage team and public shares
- Recover content owned by deleted users

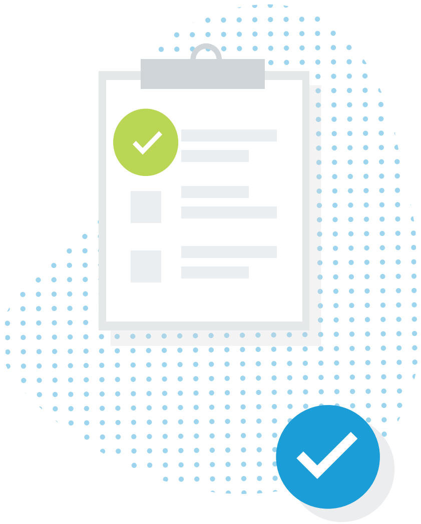
Ransomware Detection and Recovery

Datto Workplace has built-in, sophisticated **Ransomware Detection and Recovery.** As files are updated on devices, they are monitored and analyzed for possible ransomware as they are synced with the Workplace service. The overall set of file operations from devices are further analyzed on the service, and algorithms are employed to precisely identify ransomware attacks. Once an attack is identified, the affected device is quarantined to prevent the synchronization of encrypted files to other devices on the team. Administrators are immediately alerted, allowing them to respond rapidly and to revert the affected files to their last known good state, thus minimizing the impact of the ransomware attack.

Reporting

Beyond privacy-oriented security features such as encryption, access policies, and account management, **Workplace implements a set of advanced reporting capabilities specifically designed to support auditing for company policy compliance.** These advanced reporting features enable administrators to generate, export, and schedule custom reports in order to establish audit trails and analytics on the following:

- **Team Events** - Account management events for all users and groups
- **User Access Events** - Device access, PC access, user logins, IP address mapping
- **Project Events** - All changes to any projects, folders, or files
- **Device Events** - All events associated with devices connected to your Datto Workplace team



In addition, there are a number of preconfigured Special Reports, including:

- **Shares Report** - All team projects and shares permissions by users and groups, including the access level
- **Public Share Report** - All active public shares, including configuration settings
- **User Report** - All users, their roles, storage quota, creation timestamp, and last login
- **Device Report** - All devices by user, device type, OS version, app versions, last login timestamp, and when they were installed and last connected

Reports can be customized, filtered, scheduled, sent to specified users and may include or exclude a variety of events based upon selected criteria such as date range, user, device type, file name, IP address, method of access, and more. Reports can either be viewed on screen or exported to XLSX format. Reports on user access are mapped to specific source IP addresses and can be viewed on a geographical map.