Federating Google Cloud with Active Directory: Configuring single sign-on

This tutorial is the third part of a multi-part series that discusses how to extend an existing Active Directory–based identity management solution to Google Cloud. The tutorial shows how to set up single sign-on between your Active Directory (https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/active-directory-domain-services) environment and Google Cloud by using Cloud Identity (/identity), Microsoft Active Directory Federation Services (https://docs.microsoft.com/en-us/windows-server/identity/active-directory-federation-services) (AD FS), and SAML Federation (https://www.oasis-open.org/standards#samlv2.0).

The series consists of these parts:

- Federating Google Cloud with Active Directory: Introduction (/solutions/federating-gcp-with-active-directory-introduction)
- Federating Google Cloud with Active Directory: Synchronizing user accounts (/solutions/federating-gcp-with-active-directory-synchronizing-user-accounts)
- Federating Google Cloud with Active Directory: Configuring single sign-on (this tutorial)

This tutorial assumes that you understand how Active Directory identity management can be extended to Google Cloud (/solutions/federating-gcp-with-active-directory-introduction) and have already configured account synchronization between Active Directory and Cloud Identity (/solutions/federating-gcp-with-active-directory-synchronizing-user-accounts). The tutorial also assumes that you have a working AD FS 4.0 server that is running on Windows Server 2016.

To follow this tutorial, knowledge of Active Directory Domain Services and AD FS is required. You also need a user account in Cloud Identity that has super admin (https://support.google.com/cloudidentity/answer/2405986?hl=en) privileges and an account in Active Directory that has administrative access to your AD FS server.

Objectives

- Configure your AD FS server so that Cloud Identity can use it as an identity provider.

- Create a claims issuance policy that matches identities between Active Directory and Cloud Identity.
- Configure Cloud Identity so that it delegates authentication to AD FS.

Before you begin

1. Verify that your AD FS server runs Windows Server 2016 or later. While you can also configure single sign-on by using previous versions of Windows Server and AD FS, the necessary configuration steps might be different from what this tutorial describes.
2. Make sure you understand how Active Directory identity management can be extended to Google Cloud (/solutions/federating-gcp-with-active-directory-introduction).
3. Configure account synchronization between Active Directory and Cloud Identity (/solutions/federating-gcp-with-active-directory-synchronizing-user-accounts).
4. Ensure that your AD FS server uses a valid Secure Sockets Layer (SSL) certificate that the browsers of your corporate users recognize.
5. Consider setting up AD FS in a server farm configuration in order to avoid it becoming a single point of failure. After you've enabled single sign-on, the availability of AD FS determines whether users can log in to the Cloud Console.
6. If you suspect that any of the domains you plan to use for Cloud Identity could have been used by employees to register consumer accounts, consider migrating these accounts first. For more details, see migrating consumer accounts (/solutions/migrating-consumer-accounts-to-cloud-identity-or-g-suite).

Understanding single sign-on

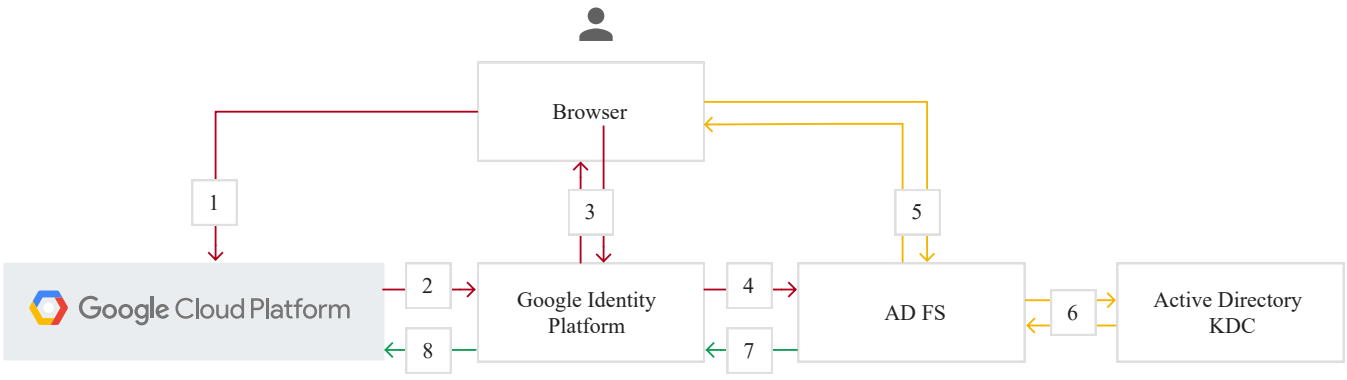
Google Cloud uses Google accounts for authentication and access management. To be able to access any Google Cloud resources, an employee needs a Google identity. Using Cloud Directory Sync (https://tools.google.com/dlpage/dirsync/), you've already automated the creation and maintenance of Google accounts and tied their lifecycle to the accounts in Active Directory.

Although Cloud Directory Sync synchronizes account details, it doesn't synchronize passwords. Whenever a user needs to authenticate in Google Cloud, the authentication must be delegated back to Active Directory, which is done by using AD FS and the Security Assertion Markup Language (SAML) protocol. This setup ensures that only Active Directory has access to user credentials and is enforcing any existing policies or multi-factor authentication (MFA) mechanisms. Moreover, it establishes a single sign-on experience between your on-premises environment and Google.

SAML 2.0 defines a protocol and an XML dialect that you can use to implement single sign-on between two parties, which are called the *identity provider* (IdP) and the *service provider* (SP):

- The SP is the party that must authenticate a user. Because it is not configured to perform this authentication itself, the SP delegates the responsibility of performing the authentication to the IdP.
- The IdP is the party that performs the user authentication. It identifies facts about the user and relays these facts back to the SP. The collection of facts is called an *assertion*.

To implement single sign-on between Active Directory and Google, you configure AD FS to act as the IdP and Cloud Identity to act as the SP. With this setup in place, signing in to the Cloud Console works as follows:



1. The user opens the Cloud Console with a browser.
2. Because the user has not been authenticated yet, the Cloud Console redirects the browser to Cloud Identity.

3. The user sees a sign-in page that asks them to enter an email address.
4. After the user submits the email address, Google Sign-In recognizes that the email address belongs to a Cloud Identity directory that has been configured for federated authentication by using AD FS. Consequently, it redirects the browser to AD FS.
5. Depending on how AD FS is configured, AD FS might return the user to the sign-in page and require that a username and password be provided. If Kerberos-based authentication is used, the user is authenticated automatically without having to enter credentials.
6. If the user has to enter credentials, AD FS interacts with the Active Directory Key Distribution Center by using Kerberos to validate username and password.
7. After successfully validating credentials, AD FS directs the browser back to Google Sign-In.
8. Google Sign-In establishes a session and sends the browser back to the Cloud Console, which now grants access.

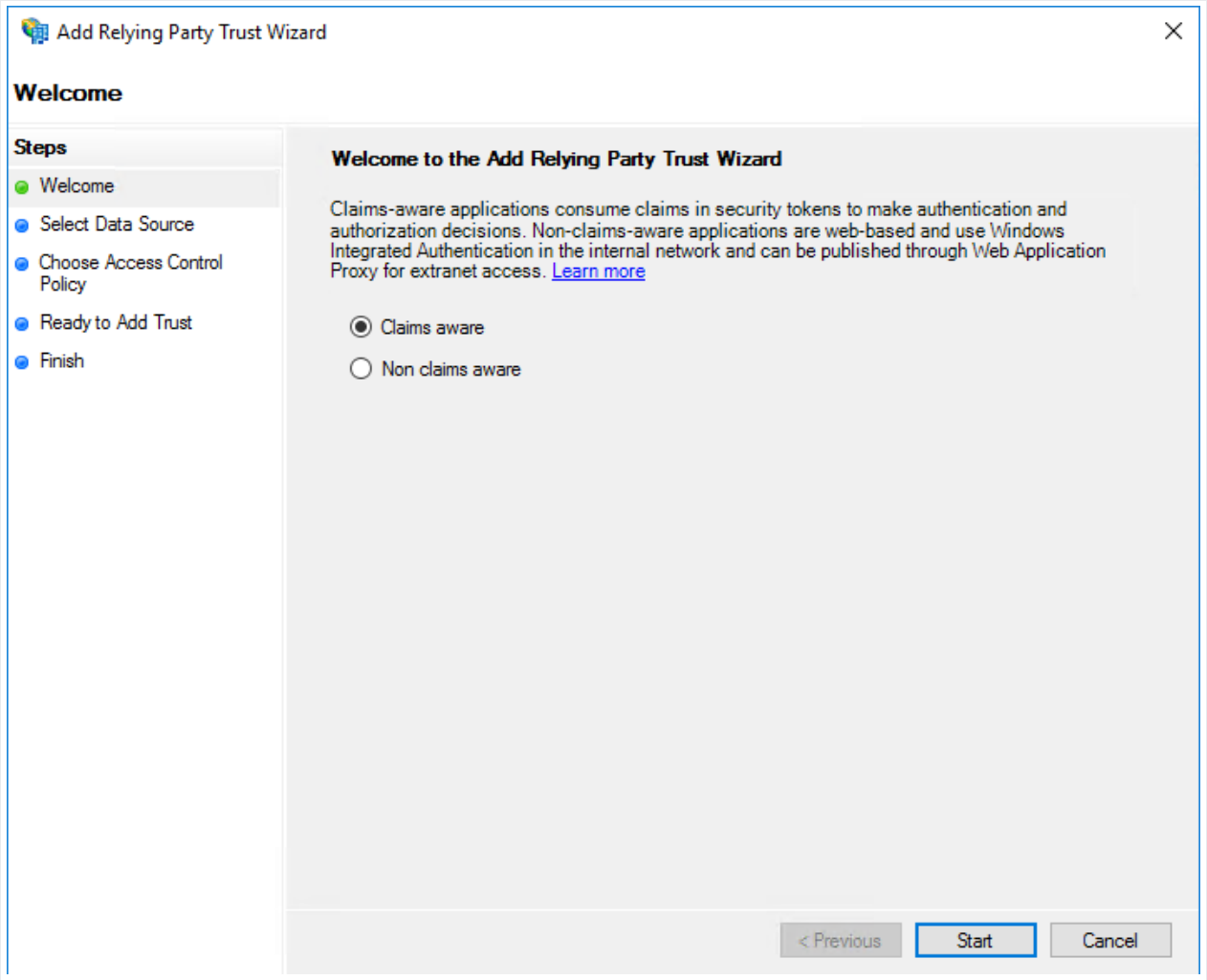
Configuring AD FS

Before enabling single sign-on in Cloud Identity, you must first configure AD FS.

Creating the relying party trust

AD FS requires that you create a *relying party trust* for each SP that is supposed to use AD FS for authentication. You start by creating a relying party trust for Cloud Identity, which involves the following:

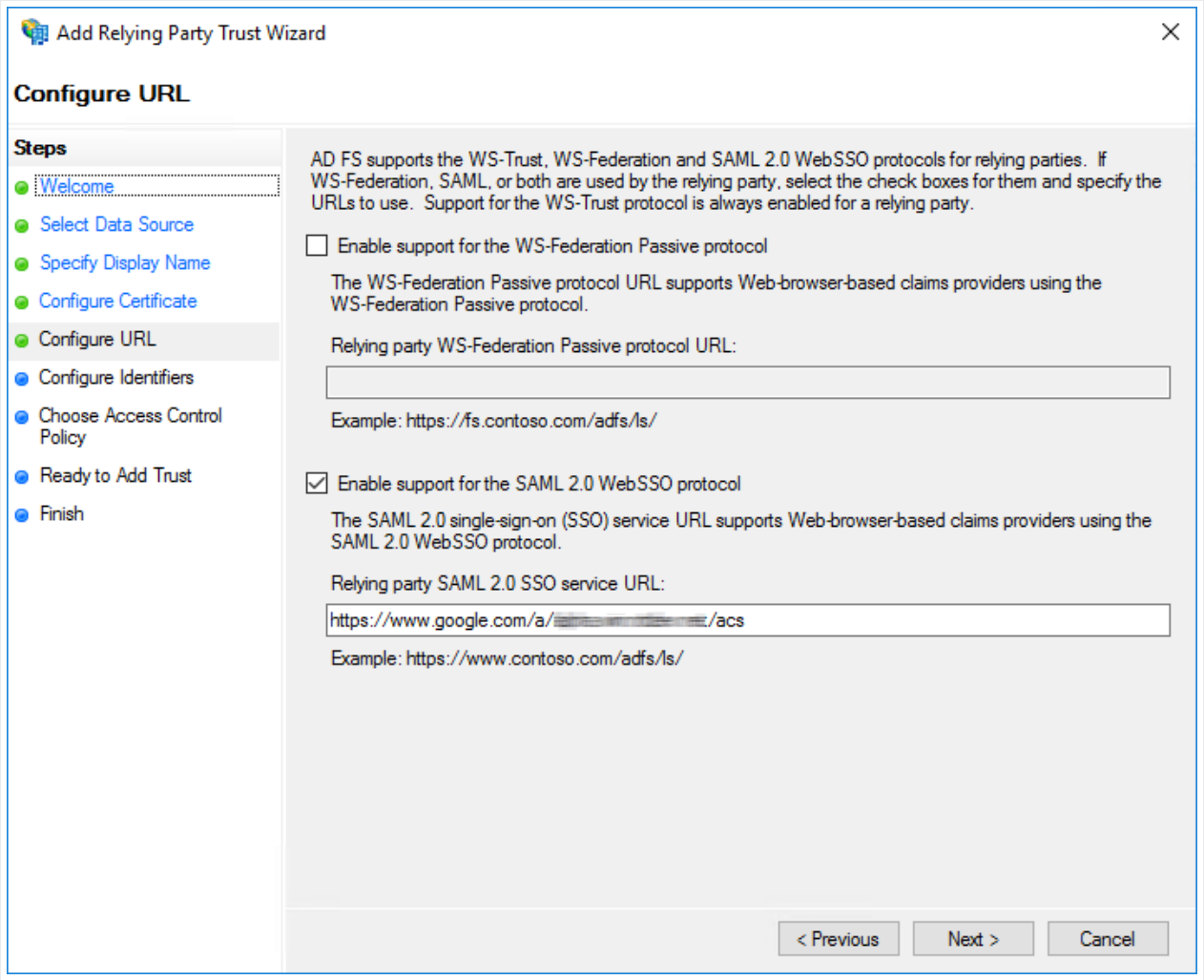
1. Log in to your AD FS server and open the AD FS MMC snap-in.
2. In the menu at left, right-click the **Relying Party Trusts** folder. In the context menu, select **Add Relying Party Trust**.
3. On the first page of the wizard, select **Claims aware**, and click **Start**.



4. On the next page, select **Enter data about the relying party manually**, and click **Next**.
5. On the next page, enter a display name such as **Cloud Identity**, and click **Next**.
6. The next page prompts you for a token encryption certificate. This step is not required in order to connect with Cloud Identity, so click **Next**.
7. On the following page, select **Enable support for the SAML 2.0 WebSSO protocol**, and enter the following SSO service URL:

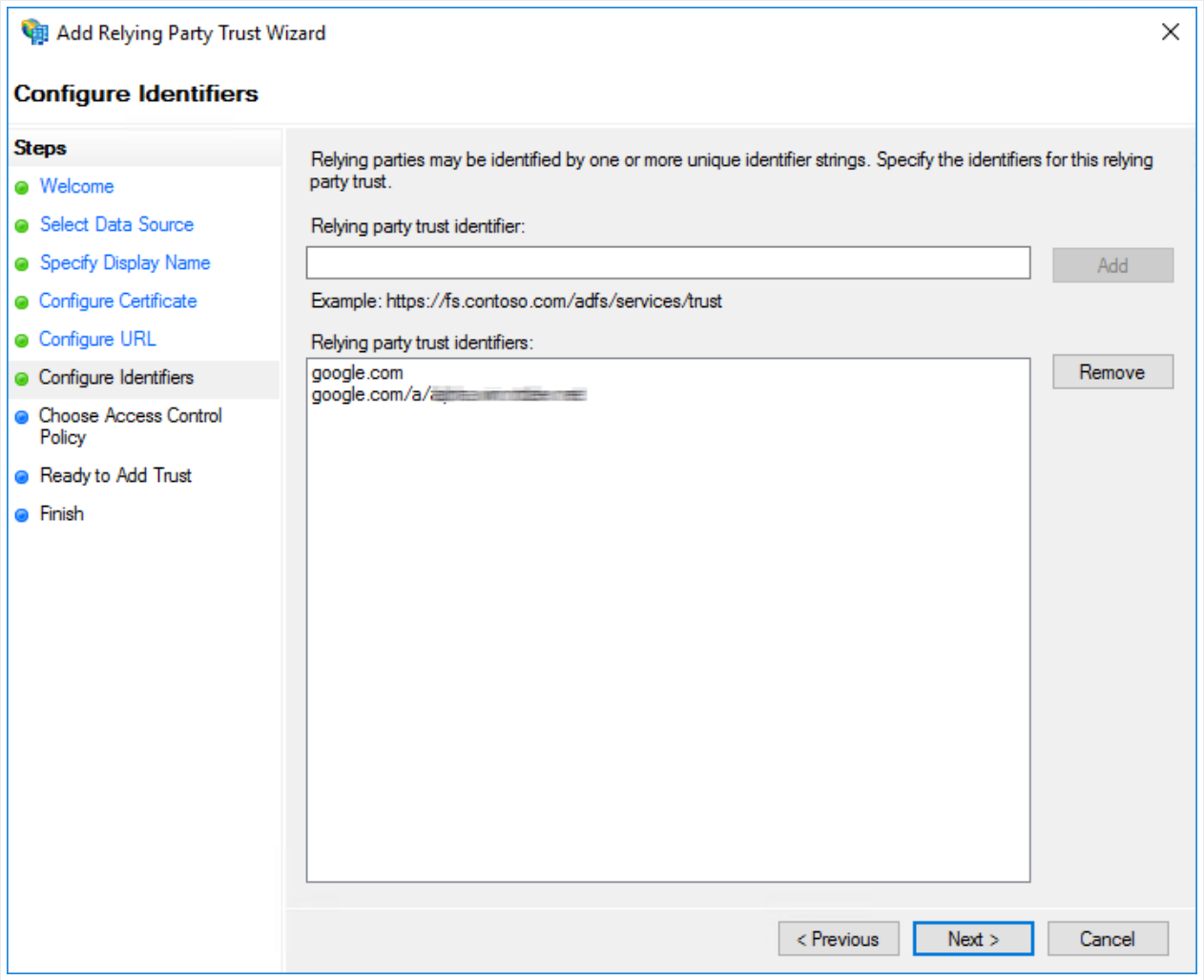
   ```
   https://www.google.com/a/[DOMAIN]/acs
   ```

   Replace `[DOMAIN]` with the *primary domain* of your Cloud Identity directory, and click **Next**.



8. The next wizard page prompts you for relying party trust identifiers. Add the following identifiers to the list:

    - `google.com/a/[DOMAIN]`, replacing `[DOMAIN]` with the primary domain of your Cloud Identity directory
    - `google.com`



Click **Next**.

9. On the next page, choose an access policy. Configuring MFA is beyond the scope of this tutorial, so click **Permit everyone** for now, and then click **Next**.
10. On the **Ready to Add Trust** page, review your settings, and then click **Next**.
11. On the final page, clear the **Configure claims issuance policy** checkbox and close the wizard. In the list of relying party trusts, you now see a new entry.

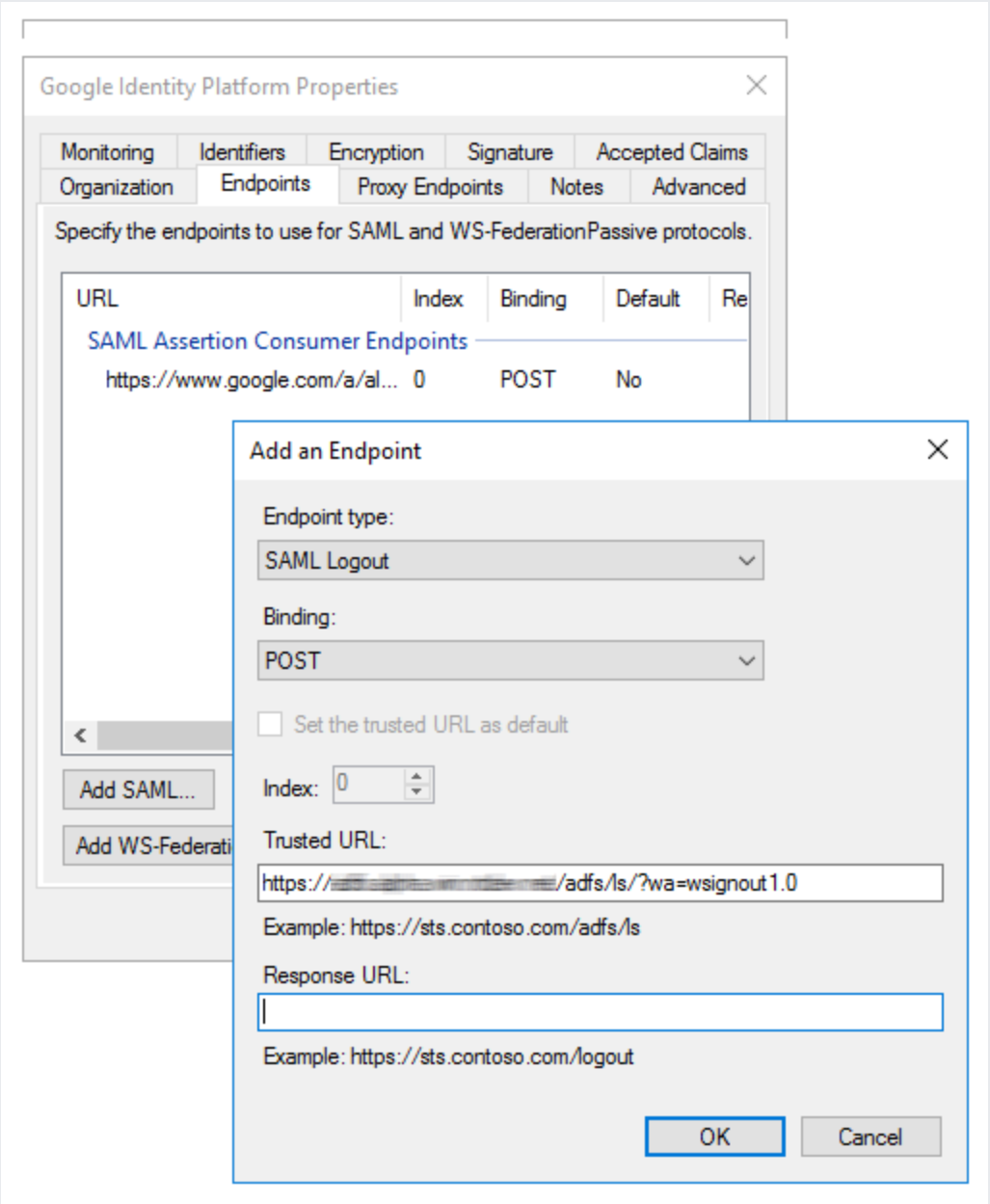
Configuring the logout URL

When you're enabling users to use single sign-on across multiple applications, it's important to allow them to sign out across multiple applications:

1. In the AD FS Management console, under **Relying Party Trusts**, right-click the trust that you just created, and click **Properties**.

2. On the **Endpoints** tab, click **Add SAML**.
3. In the **Add an Endpoint** dialog, configure the following settings:
    a. **Endpoint type**: **SAML Logout**
    b. **Binding**: **POST**
    c. **Trusted URL**: `https://[ADFS]/adfs/ls/?wa=wsignout1.0`

    Replace `[ADFS]` with the fully qualified domain name of your AD FS server.



4. Click **OK**.

5. Click **OK** to close the dialog.

Configuring the claims mapping

After AD FS has authenticated a user, it issues a SAML assertion to Cloud Identity. This assertion serves as proof that authentication has successfully taken place. The assertion must identify who has been authenticated, which is the purpose of the NameID claim (https://support.google.com/a/answer/6330801?hl=en).

For Cloud Identity to map the NameID to the associated user account, the NameID must contain the corresponding email address. Depending on how you are mapping account identities (/solutions/federating-gcp-with-active-directory-introduction#mapping_account_identities) between Active Directory and Cloud Identity, the NameID must contain the UPN or the email address from the Active Directory account, with domain substitutions applied as necessary.

UPNUPN: domain substitution (#upn:-dorEmail (#email)Email: domain substitution (#email:-c

1. In the AD FS Management console, under **Relying Party Trusts**, right-click the newly created trust, and click **Edit Claim Issuance Policy**.
2. In the dialog, click **Add Rule**.
3. Select **Send LDAP Attributes as Claims**, and click **Next**.
4. On the next page, apply the following settings:
    a. **Claim rule name**: **Map Email and Name ID**
    b. **Attribute Store**: **Active Directory**
5. Add a row to the list of LDAP attribute mappings:
    a. **LDAP Attribute**: `User-Principal-Name`
    b. **Outgoing Claim Type**: `Name ID`
6. Click **Finish**, and then click **OK**.

Exporting the AD FS token-signing certificate

When AD FS issues a SAML assertion to Cloud Identity, Cloud Identity *must* verify the integrity and authenticity of the assertion. For this purpose, SAML requires that the assertion be signed using a special *token-signing key*, which is the private key of a designated public/private key

pair. The public key of this pair is made available to SPs in the form of a *token-signing certificate* and enables SPs to verify the signature of an assertion.

Before configuring Cloud Identity, you must export the token-signing certificate from AD FS:

1. In the AD FS Management console, click **Service** > **Certificates**.
2. Right-click the certificate that is listed under **Token-signing**, and click **View Certificate**.
3. Click the **Details** tab.
4. Click **Copy to File** to open the Certificate Export Wizard.
5. Click **Next**.
6. Select **DER encoded binary X.509 (.CER)** as format, and click **Next**.
7. Provide a local filename, and click **Next**.
8. Confirm the export by clicking **Finish**.
9. Click **OK** to dismiss the message box confirming that the export was successful.
10. Copy the exported certificate to your local computer.

Configuring Cloud Identity

With the AD FS configuration completed, you can now configure single sign-on in Cloud Identity:

1. In the Admin console (http://admin.google.com/), click **Security** > **Settings**.
2. Click **Set up single sign-on (SSO) with a third party IdP**.
3. Ensure that **Setup SSO with third party identity provider** is enabled.
4. Enter the following settings. In all URLs, replace `[ADFS]` with the fully qualified domain name of your AD FS server:
    a. **Sign-in page URL**: `https://[ADFS]/adfs/ls/`
    b. **Sign-out page URL**: `https://[ADFS]/adfs/ls/?wa=wsignout1.0`
    c. **Change password URL**: `https://[ADFS]/adfs/portal/updatepassword/`

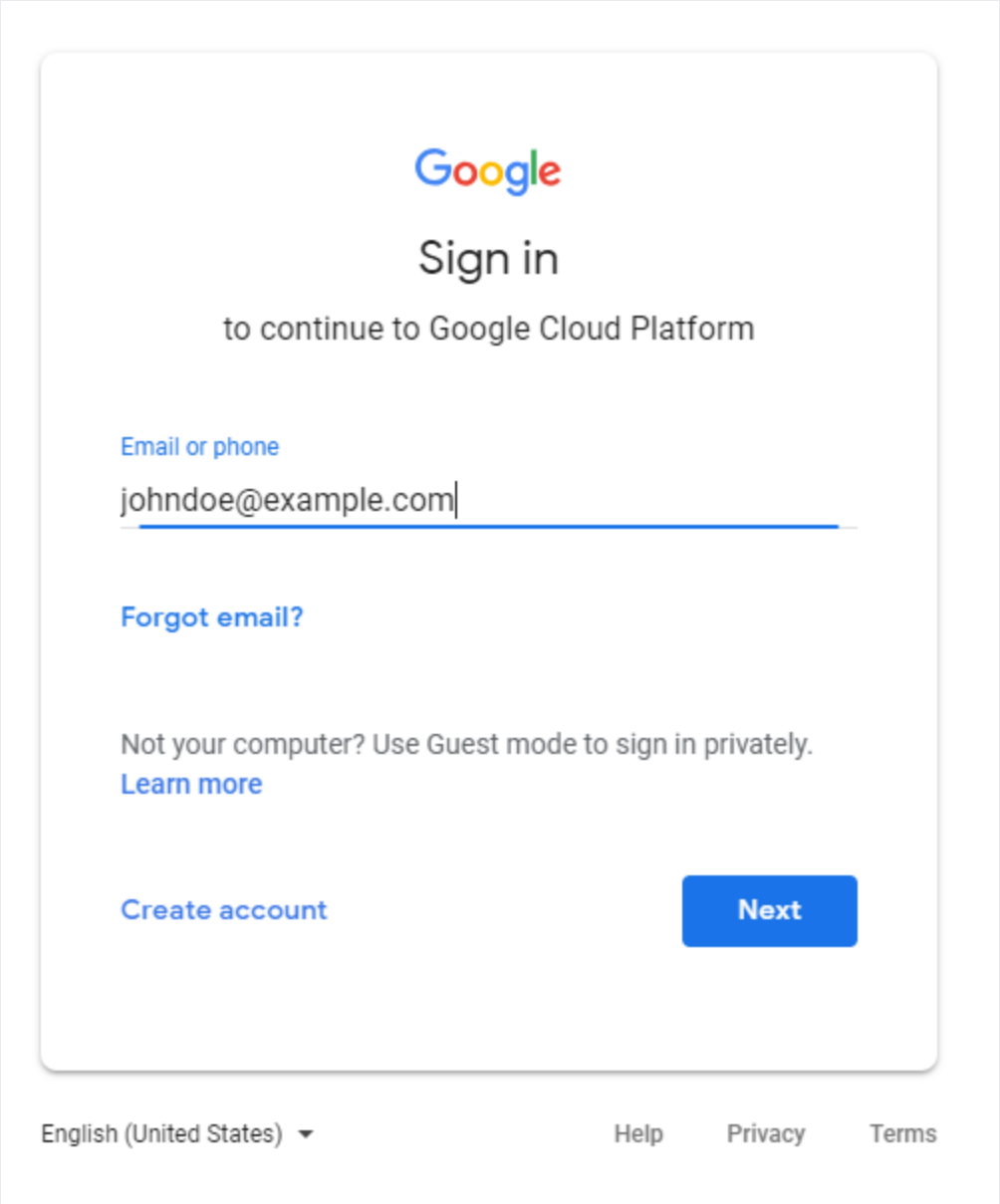
5. Under **Verification certificate**, click **Choose File**, and pick the AD FS token-signing certificate that you downloaded previously.
6. Click **Save**.
7. On the next page, confirm that you intend to enable single sign-on, and click **I understand and agree**.
8. To sign out of the Admin console, at the upper right, click the avatar, and then click **Sign out**.

Note: The token-signing certificate is valid for a limited period of time. Depending on your configuration (https://docs.microsoft.com/en-us/windows-server/identity/ad-fs/operations/configure-ts-td-certs-ad-fs), AD FS either renews the certificate automatically before it expires, or it requires you to provide a new certificate before the current certificate expires. In both cases, you must update the Cloud Identity configuration to use the new certificate.

Testing single sign-on

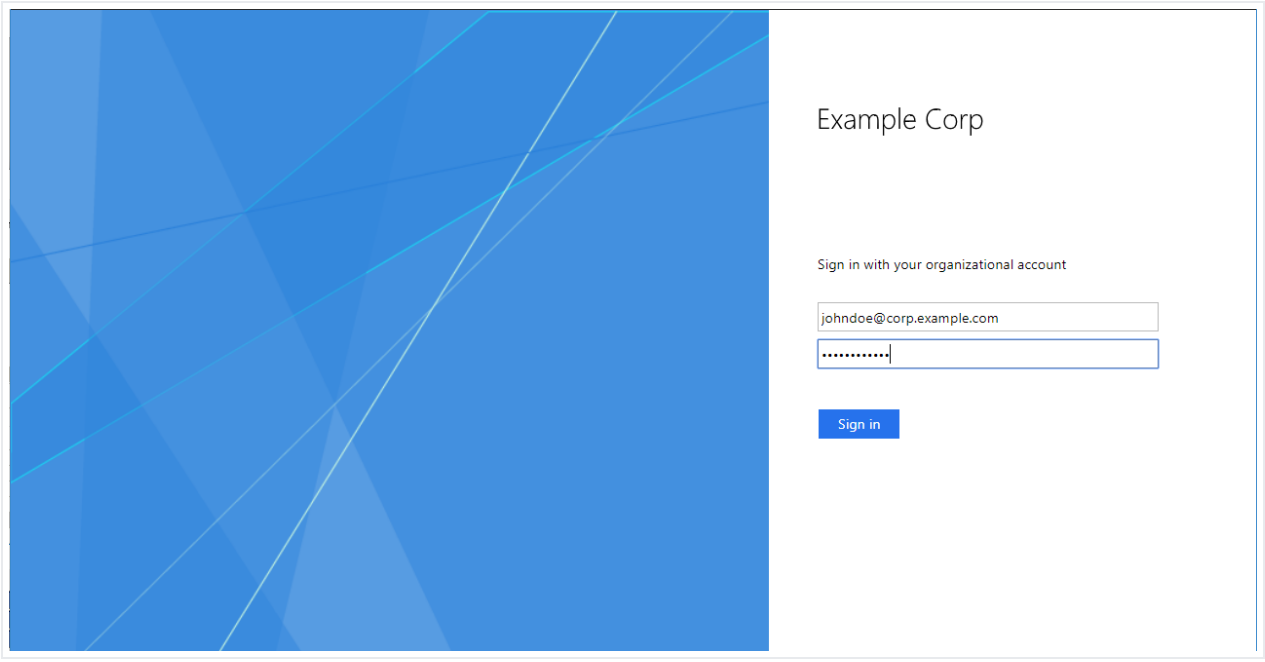
You've now completed the single sign-on configuration in both AD FS and Cloud Identity. To check if single sign-on works as intended, run the following test:

1. Choose an Active Directory user account that has previously been synchronized to Cloud Identity and does not have super admin privileges assigned. User accounts that have super admin privileges must always sign in by using Google credentials, so they aren't suitable for testing single sign-on.
2. Open a new browser window and navigate to https://console.cloud.google.com/ (https://console.cloud.google.com/).
3. On the Google Sign-In page that appears, enter the email address of the user account, and click **Next**. If you use domain substitution, you must apply the substitution to the email address.



You are redirected to AD FS. If you configured AD FS to use forms-based authentication, you now see the sign-in page.

4. Enter your UPN and password for the Active Directory account, and click **Sign in**.



5. After successful authentication, AD FS redirects you back to Google Identity Platform. Because this is the first login for this user, you're asked to accept the Google terms of service and privacy policy.
6. If you agree to the terms, click **Accept**.
7. You are redirected to the Cloud Console, which asks you to confirm preferences and accept the Google Cloud terms of service. If you agree to the terms, click **Yes**, and then click **Agree and Continue**.
8. At the upper left, click the avatar icon, and click **Sign out**.

   You are then redirected to an AD FS page confirming that you've been successfully signed out.

If you have trouble signing in, enabling the AD FS debug log (https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2008-R2-and-2008/ff641696(v=ws.10)) on the AD FS server can help you diagnose the issue. If you're using Integrated Windows Authentication, consider temporarily switching to forms-based authentication so that you can perform tests with different user accounts more easily.

Keep in mind that user accounts that have super admin privileges are exempted from single sign-on, so you can still use the Admin console to verify or change settings.

Cleaning up

If you don't intend to keep single sign-on enabled for your organization, follow these steps to disable single sign-on in Cloud Identity:

1. In the Admin console (http://admin.google.com/), click **Security** > **Settings**.
2. Click **Set up single sign-on (SSO) with a third party IdP**.
3. Clear the **Setup SSO with third party identity provider** checkbox.
4. Click **Save**.

To clean up configuration in AD FS, follow these steps:

1. Log in to your AD FS server and open the **AD FS** MMC snap-in.
2. In the menu at left, right-click the **Relying Party Trusts** folder.
3. In the list of relying party trusts, right-click **Cloud Identity**, and click **Delete**.
4. Confirm the deletion by clicking **Yes**.

What's next

- Learn more about Cloud IAM (/iam/docs/overview).
- Read about best practices for setting up an enterprise organization in Google Cloud (/docs/enterprise/best-practices-for-enterprise-organizations).
- Try out other Google Cloud features for yourself. Have a look at our tutorials (/docs/tutorials).

Last updated 2020-04-20.