Setting up SSO

You can set up SSO with Google as your service provider in a number of ways, depending on your organization's needs. Google Workspace supports both SAML-based and OIDC-based SSO.

- SSO **profiles**, which contain the settings for your IdP, give you the flexibility to apply different SSO settings to different users in your organization. Create SAML-based profiles (#create_profile), custom OIDC profiles (#create_OIDC_profile), or use the default Microsoft Entra OIDC profile (#OIDC_setup), which needs no configuration.
- After creating SSO profiles, assign profiles to organization units or groups (#assign_profile) to set the IdP for those users. You can also turn off SSO for specific organization units or groups.

If your users use **domain-specific service URLs** to access Google services (for example, https://mail.google.com/a/example.com), you can also manage how these URLs work with SSO (/admin/apps/optional-sso-settings-and-maintenance#service_URLs).

If your organization needs conditional SSO redirection based on IP address, or SSO for super admins, you also have the option to configure the legacy SSO profile (#legacy_profile).

Set up SSO with SAML

Before you begin

To set up a SAML SSO profile, you'll need some basic configuration from your IdP's support team or documentation:

- **IdP entity ID**: This is how your IdP identifies itself when communicating with Google.
- **Sign-in page URL**: This is also known as the SSO URL or SAML 2.0 Endpoint (HTTP). This is where users sign in to your IdP.
- **Sign-out page URL**: The page where the user lands after exiting the Google app or service.
- **Change password URL**: The page where SSO users will go to change their password (instead of changing their password with Google).

- **Certificate**: The X.509 PEM certificate from your IdP. The certificate contains the public key that verifies sign-in from the IdP.

> Certificate requirements
>
> - The certificate must be a PEM or DER formatted X.509 certificate with an embedded public key.
> - The public key must be generated with the DSA or RSA algorithms.
> - The public key in the certificate must match the private key used to sign the SAML response.
>
> You'll usually get these certificates from your IdP. However, you can also generate them yourself (/admin/apps/generate-keys-and-certificates-for-sso).

Create a SAML SSO profile

Follow these steps to create a third-party SSO profile. You can create up to 1,000 profiles in your organization.

1. In the Google Admin console, go to Menu
   Security
   Authentication
   SSO with third party IdP.

   Go to SSO with third party IdP (https://admin.google.com/ac/security/sso)

   Requires having the Security Settings administrator privilege (/admin/users/administrator-privilege-definitions#user_security).
2. In the **Third-party SSO profiles** section, click **Add SAML profile**.
3. For **SAML SSO profile**, enter a profile name.
4. (Optional) For **Autofill email**, select the option that matches your IdP's supported login hint format. For details, go to Use Autofill email to simplify SSO sign-ins

(/admin/apps/optional-sso-settings-and-maintenance#autofill).

5. In the **IdP details** section, complete the following steps:
    a. Enter the **IDP entity ID**, **Sign-in page URL**, and **Sign-out page URL** that you got from your IdP.
    b. For **Change password URL**, enter a change password URL for your IdP. Users will go to this URL to reset their passwords.
6. Click **Upload certificate**.

    You can upload up to two certificates, giving you the option to rotate certificates (/admin/apps/optional-sso-settings-and-maintenance#rotate_certificate) when necessary.
7. Click **Save**.
8. In the **SP Details** section, copy and save the **Entity ID** and **ACS URL**. You'll need these values to configure SSO with Google in your IdP admin control panel.
9. (Optional) If your IdP supports encrypting assertions, you can generate and share a certificate with your IdP to turn on encryption. Each SAML SSO profile can have up to 2 SP certificates.
    a. Click the **SP Details** section to enter edit mode.
    b. For **SP certificate**, click **Generate certificate**.
    c. Click **Save**. Copy the certificate contents or download it as a file.
    d. Share the certificate with your IdP.
    e. (Optional) To rotate a certificate, return to **SP Details** and click **Generate another certificate**, then share the new certificate with your IdP. Once you're sure your IdP is using the new certificate, delete the original certificate.

Configure your IdP

To configure your IdP to use this SSO profile, enter the information from the **Service Provider (SP) Details** section of the profile into the appropriate fields in your IdP SSO settings. Both the ACS URL and Entity ID are unique to this profile.

> Configure the legacy SSO profile

The legacy SSO profile is supported for users who have not migrated to SSO profiles. It only supports usage with a single IdP.

1. In the Google Admin console, go to Menu
   Security
   Authentication
   SSO with third party IdP.

   Go to SSO with third party IdP (https://admin.google.com/ac/security/sso)

   Requires having the Security Settings administrator privilege (/admin/users/administrator-privilege-definitions#user_security).
2. In **Third-party SSO profiles**, click **Add SAML profile**.
3. At the bottom of the **IdP details** page, click **Go to legacy SSO profile setting**s.
4. On the **Legacy SSO profile** page, check the **Enable SSO with third-party identity provide**r box.
5. Fill in the following information for your IdP:
   - Enter the **Sign-in page URL** and **Sign-out page URL** for your IdP.

     Note: All URLs must be entered and must use HTTPS, for example https://sso.example.com.
   - Click **Upload certificate** and locate and upload the X.509 certificate supplied by your IdP. For more information, see Certificate requirements (#certificate_requirements).
   - Choose whether to use a **domain-specific issuer** in the SAML request from Google.

     If you have multiple domains using SSO with your IdP, use a domain-specific issuer to identify the correct domain issuing the SAML request.

     - **Checked** Google sends an issuer specific to your domain: google.com/a/example.com (where *example.com* is your primary Google Workspace domain name)

- **Unchecked** Google sends the standard issuer in the SAML request: google.com

- (Optional) To apply SSO to a set of users within specific IP address ranges, enter a network mask. For more information see Network mapping results (/admin/apps/optional-sso-settings-and-maintenance#network_mapping).

  Note: you can also set up partial SSO by assigning the SSO profile to specific organizational units or groups.

- Enter a **change password URL** for your IdP. Users will go to this URL (rather than the Google change password page) to reset their passwords. All users, other than super administrators, who try to change their password at https://myaccount.google.com/ will be directed to the URL you specify. This setting applies even if you do not enable SSO. Also, network masks do not apply.

  Note: If you enter a URL here, users are directed to this page even if you don't enable SSO for your organization.

6. Click **Save**.

After saving, the legacy SSO profile is listed in the **SSO profiles** table.

Configure your IdP

To configure your IdP to use this SSO profile, enter the information from the Service Provider (SP) Details section of the profile into the appropriate fields in your IdP SSO settings. Both the ACS URL and Entity ID are unique to this profile.

	Format
ACS URL	https://accounts.google.com/a/{*domain.com*}/acs Where *{domain.com}* is your organization's Workspace domain name
Entity ID	Either of the following: • google.com • google.com/a/*customerprimarydomain* (if you choose to use a domain-specific issuer when configuring the legacy profile).

Disable the legacy SSO profile

1. In the **Third-party SSO profiles** list, click **Legacy SSO profile**.

2. In the **Legacy SSO profile** settings, uncheck **Enable SSO with third-party identity provider**.
3. Confirm that you want to continue, then click **Save**.

In the **SSO profiles** list, the **Legacy SSO profile** now shows as **Disabled**.

- Organizational units that have the Legacy SSO profile assigned will display an alert in the **Assigned profile** column.
- The top level organizational unit will display **None** in the **Assigned profile** column.
- In **Manage SSO profile assignments**, the Legacy SSO profile shows as **inactive**.

Migrate from legacy SAML to SSO profiles

If your organization is using the legacy SSO profile, we recommend migrating to SSO profiles, which offer several advantages including OIDC support, more modern APIs, and greater flexibility in applying SSO settings to your user groups. Learn more (/admin/apps/migrating-from-legacy-sso-to-sso-profiles).

Set up SSO with OIDC

Follow these steps to use OIDC-based SSO:

1. Choose an OIDC option—either create a **custom OIDC profile**, where you provide information for your OIDC partner, or use the pre-configured Microsoft Entra OIDC profile.
2. Follow the steps in Decide which users should use SSO (#assign_profile) to assign the pre-configured OIDC profile to selected organizational units/groups.

If you have users within an organizational unit (for example in a sub-organizational unit) who *don't need* SSO, you can also use assignments to turn SSO off for those users.

Note: The Google Cloud Command Line Interface (https://cloud.google.com/cli) does not currently support reauthentication with OIDC.

Before you begin

To set up a custom OIDC profile, you'll need some basic configuration from your IdP's support team or documentation:

- **Issuer URL** The complete URL of the IdP authorization server.
- An OAuth client, identified by its **Client ID** and authenticated by a **Client secret**.
- **Change password URL** The page where SSO users will go to change their password (instead of changing their password with Google).

Also, Google needs your IdP to do this:

- The `email` claim from your IdP must match the user's primary email address on the Google side.
- It must use the authorization code flow.

Create a custom OIDC profile

1. In the Google Admin console, go to Menu
   Security
   Authentication
   SSO with third party IdP.

   Go to SSO with third party IdP (https://admin.google.com/ac/security/sso)

   Requires having the Security Settings administrator privilege (/admin/users/administrator-privilege-definitions#user_security).
2. In **Third-party SSO profiles**, click **Add OIDC profile**.
3. Name the OIDC profile.
4. Enter OIDC details: Client ID, Issuer URL, Client secret.
5. Click **Save**.
6. On the OIDC SSO settings page for the new profile, copy the **Redirect URI**. You'll need to update your OAuth client on your IdP to respond to requests using this URI.

To edit settings, hover over the **OIDC Details**, then click Edit

.

Use the Microsoft Entra OIDC profile

Make sure you've configured the following prerequisites for OIDC in your organization's Microsoft Entra ID tenant:

- The Microsoft Entra ID tenant needs to be domain verified (https://docs.microsoft.com/en-us/azure/active-directory/fundamentals/add-custom-domain).
- End users must have Microsoft 365 licenses (https://docs.microsoft.com/en-us/microsoft-365/admin/manage/assign-licenses-to-users).
- The username (primary email) of the Google Workspace admin assigning the SSO profile must match the primary email address of your Azure AD tenant admin account.

Decide which users should use SSO

Turn SSO on for an organizational unit or group by assigning an SSO profile and its associated IdP. Or, turn SSO off by assigning 'None' for the SSO profile. You can also apply a mixed SSO policy within an organizational unit or group, for example turning SSO on for the organizational unit as a whole, then turning it off for a sub-organizational unit.

If you haven't created a SAML (#create_profile) or OIDC (#create_OIDC_profile) profile, do that before continuing. Or, you can assign the preconfigured OIDC profile.

1. Click **Manage SSO profile assignments**.
2. If this is your first time assigning the SSO profile, click Get started. Otherwise, click **Manage assignments**.
3. On the left, select the organizational unit or group to which you're assigning the SSO profile.
    - If the SSO profile assignment for an organizational unit or group differs from your domain-wide profile assignment, an override warning appears when you select that organizational unit or group.

- You can't assign the SSO profile on a per-user basis. The Users view lets you check the setting for a specific user.

4. Choose an **SSO profile assignment** for the selected organizational unit or group:
    - To exclude the organizational unit or group from SSO, choose **None**. Users in the organizational unit or group will sign in directly with Google.
    - To assign another IdP to the organizational unit or group, choose **Another SSO profile**, then select the SSO profile from the dropdown list.
5. (SAML SSO profiles only) After selecting a SAML profile, choose a sign-in option for users who go directly to a Google service without first signing in to the SSO profile's third-party IdP. You can prompt users for their Google username, then redirect them to the IdP, or require users to enter their Google username and password.

    Note: If you choose to require users to enter their Google username and password, the **Change password URL** setting for this SAML SSO profile (available at SSO Profile > IDP details) is ignored. This ensures that users are able to change their Google passwords as needed.
6. Click **Save**.
7. (Optional) Assign SSO profiles to other organizational units or groups as needed.

After you close the **Manage SSO profile assignments** card, you'll see the updated assignments for organizational units and groups in the **Manage SSO profile assignments** section.

Remove an SSO profile assignment

1. Click a group or organizational unit name to open its profile assignment settings.
2. Replace the existing assignment setting with the parent organization unit setting:
    - For organizational unit assignments—click **Inherit**.
    - For group assignments—click **Unset**.

Note: Your top organizational unit is always present in the profile assignment list, even if the Profile is set to None.

See also

- Optional SSO settings and maintenance (/admin/apps/optional-sso-settings-and-maintenance)
- Troubleshoot SSO (/admin/support/troubleshooting/troubleshoot-single-sign-on-sso)
- Multi-party approval for sensitive actions (/admin/security/multi-party-approval-for-sensitive-actions)

Last updated 2026-07-17 UTC.