Stack Overflow Enterprise Documentation

Configure Single Sign-on (SSO) with Google

Set up Stack Overflow for Teams Enterprise for SAML authentication with Google.

Document generated 02/19/2025

PDF VERSION

Tags | **Authentication** | **SAML** | **SSO** | **Google** |

Applies to: Free Basic Business Enterprise

ADMIN PRIVILEGES REQUIRED

This documentation is for ***Stack Overflow for Teams Enterprise****. Free, Basic, and Business users can access their documentation here. Find your plan.*

Overview

These instructions describe how to integrate your Stack Overflow for Teams Enterprise (SOE) site with Google as your Identity Provider (IdP) for authentication. Once configured, your users will be able to use Google and the Security Assertion Markup Language (SAML) for Single Sign-on (SSO) authentication into your site. You can learn more about SAML in our SAML Authentication Overview document.

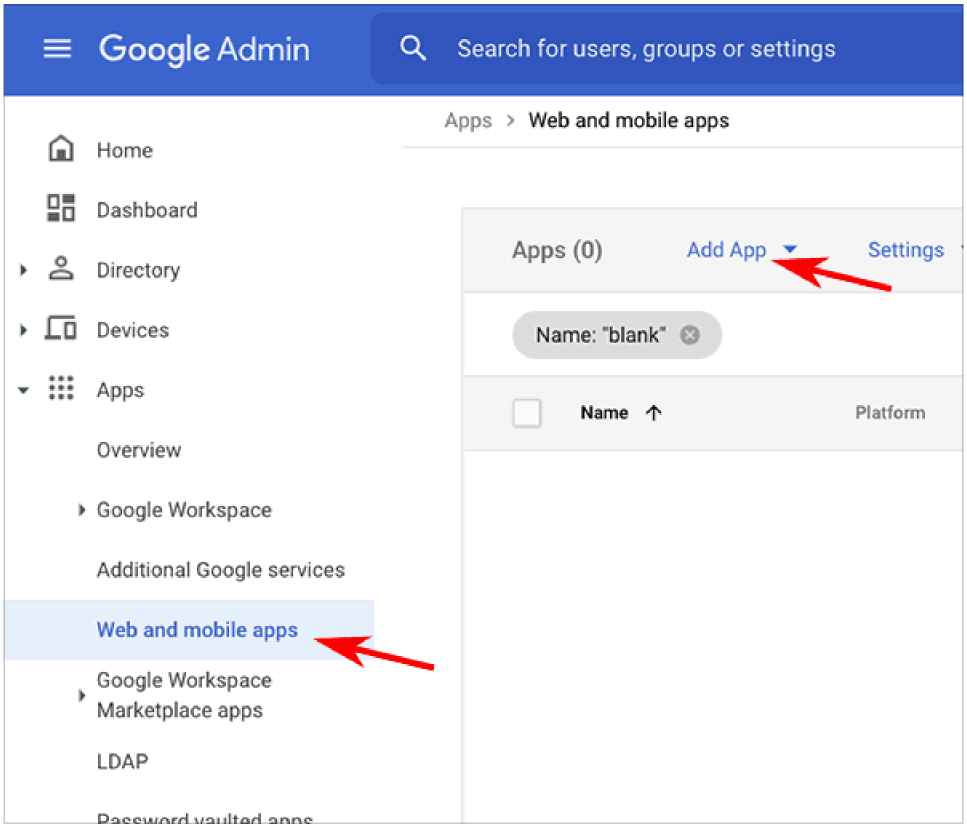
When setting up SAML authentication, you'll configure your SOE site and the Google IdP in a back-and-forth process. We recommend having a browser tab open to each site.

THIS ARTICLE APPLIES TO STACK OVERFLOW FOR TEAMS ENTERPRISE ONLY.
Other Stack Overflow for Teams users should read this article instead. Find your plan.

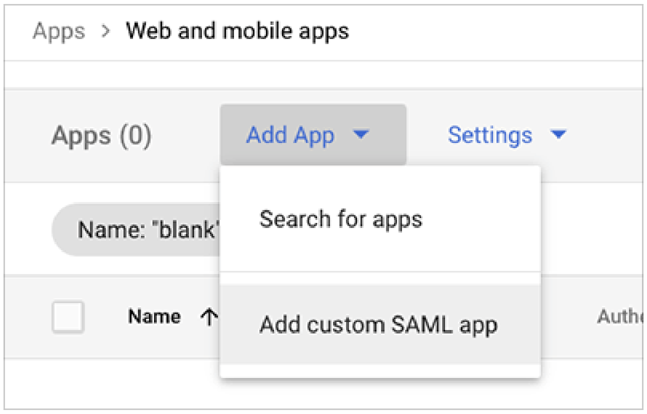
Create a new SAML application

To configure SSO with Google, start by creating a SAML application within your Google Workspace.

1. Go to your Google Admin panel.
2. Click **Apps**, then **Web and mobile apps**.
3. Click **Add App** at the top of the screen.



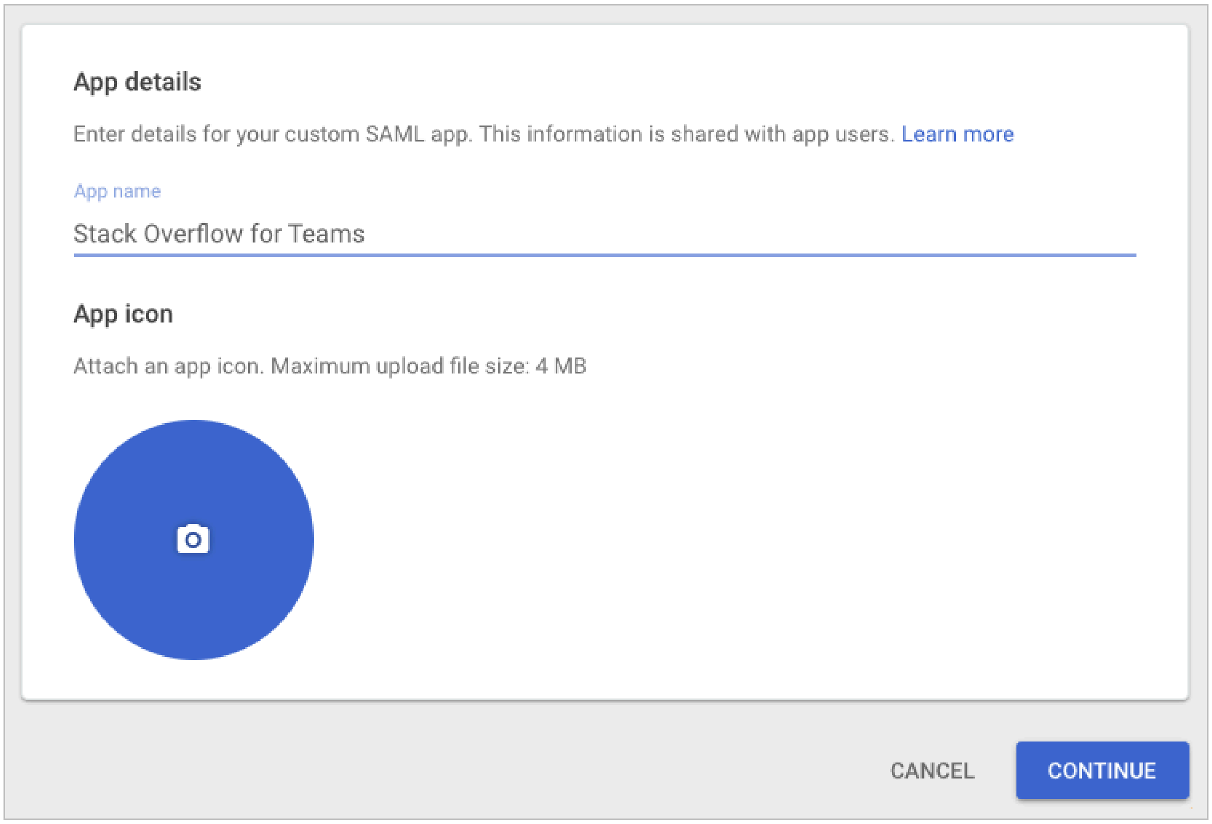
4. Click **Add custom SAML app**.



Configure the SAML Application

1. Configure the following settings in your new SAML app.

   - **App details** Give your app any name (for example: Stack Overflow for Teams). Click **CONTINUE**.



App details

Enter details for your custom SAML app. This information is shared with app users. Learn more

App name

Stack Overflow for Teams

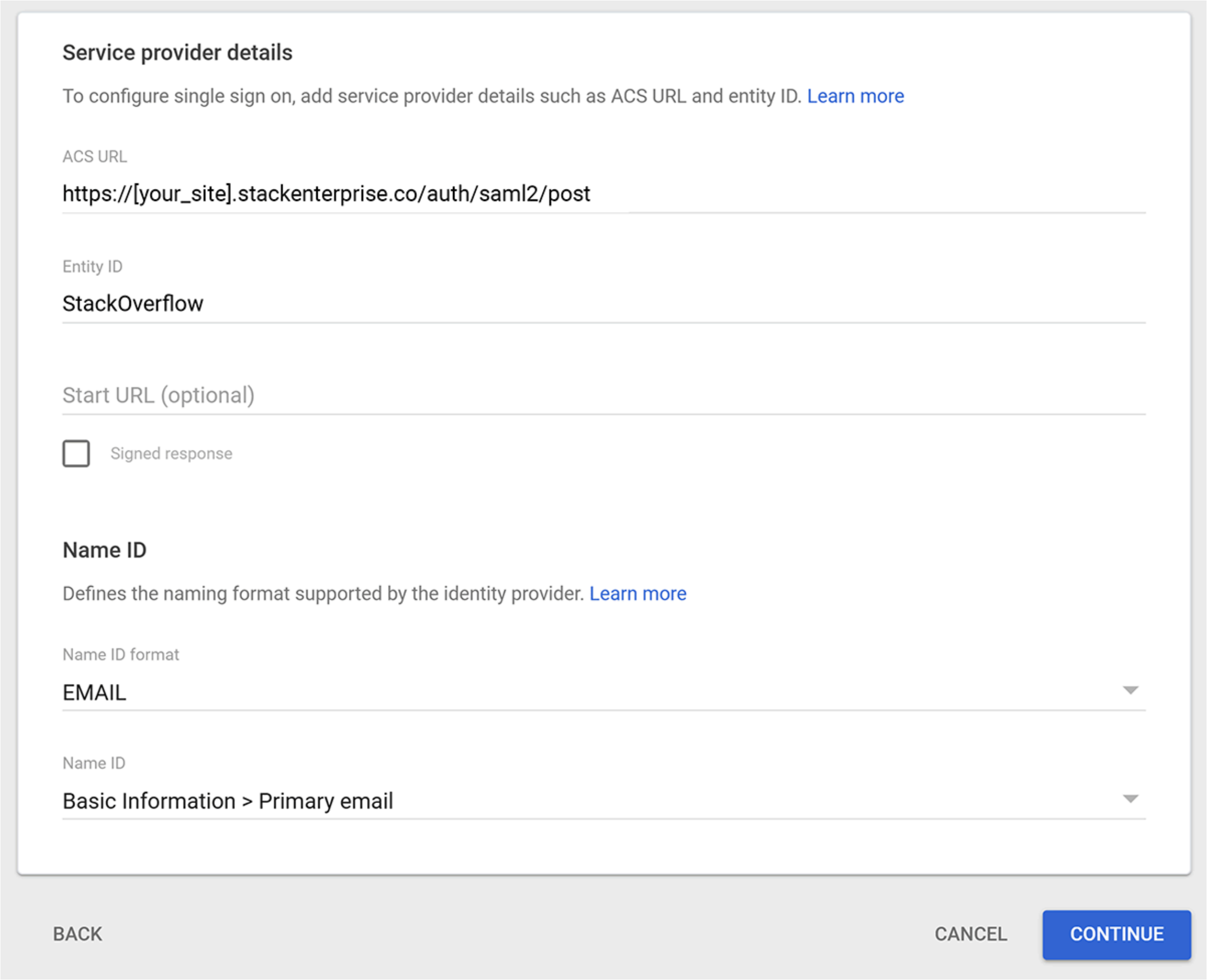
App icon

Attach an app icon. Maximum upload file size: 4 MB

Make no changes on the "Google Identity Provider details" tab. You’ll retrieve these details in a later step.

2. Configure the following settings on the "Service provider details" tab:

   - **ACS URL** Set this to **https://[your_site]/auth/saml2/post**.
   - **Entity ID** This can be any value you wish (for example: StackOverflow). You'll use this value in a later step, entering it into your SOE authentication settings as **Issuer**.
   - **Start URL** Leave this field blank.
   - **Name ID format** We recommended setting this field to **EMAIL**. Of the three options Google allows (Email, FirstName or LastName), email is most likely to be unique across all users.
   - **Name ID** Set to **Basic Information > Primary email**.



Service provider details

To configure single sign on, add service provider details such as ACS URL and entity ID. Learn more

ACS URL: https://[your_site].stackenterprise.co/auth/saml2/post

Entity ID: StackOverflow

Start URL (optional)

□ Signed response

Name ID

Defines the naming format supported by the identity provider. Learn more

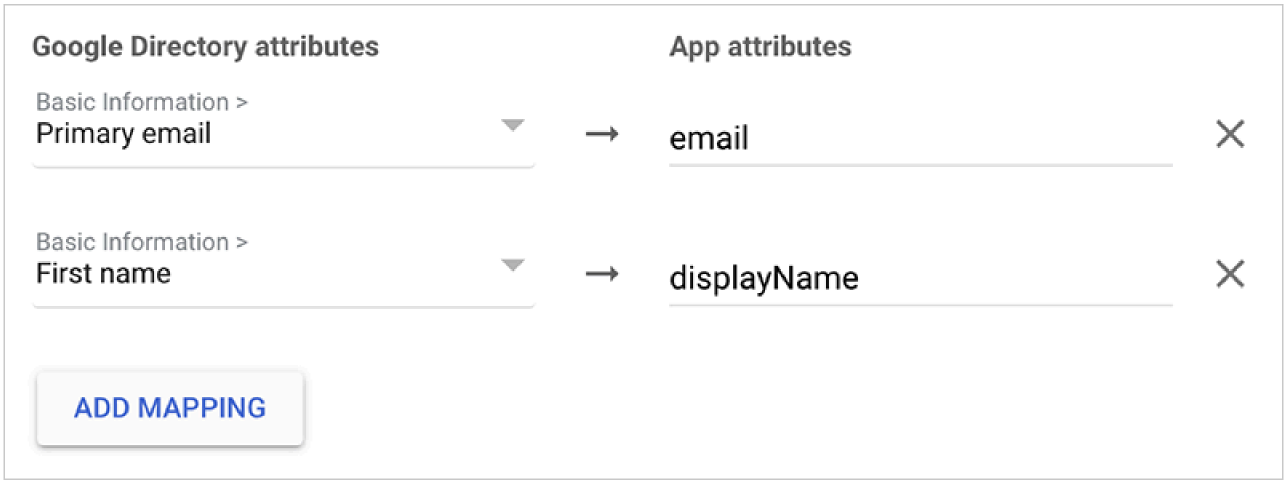
Name ID format: EMAIL

Name ID: Basic Information > Primary email

Update attribute mapping

Now you'll configure the user data Google returns with the SAML response. You need to specify at least one SAML attribute for the user display name and one for the user email. Click **ADD MAPPING** to map Google user data to the returned SAML attributes. The SAML protocol returns the attributes you configure as assertions.

Here is one recommended way to set up your attribute mapping:

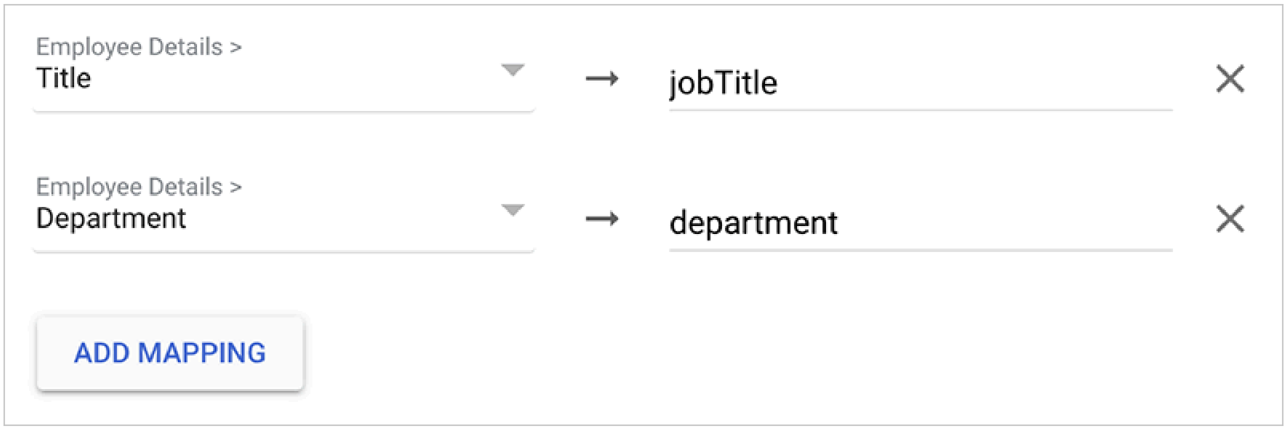


Google Directory attributes		App attributes
Basic Information > Primary email	→	email
Basic Information > First name	→	displayName

NOTE: *Full name would be a better choice for the `displayName` attribute, but Google doesn't offer this as a default field. To learn more about creating custom attributes (like full name), see the Google custom attributes guide.*

You can also add the following optional SAML attributes:

- Job Title (for example: app attribute jobTitle)
- Department (for example: app attribute department)



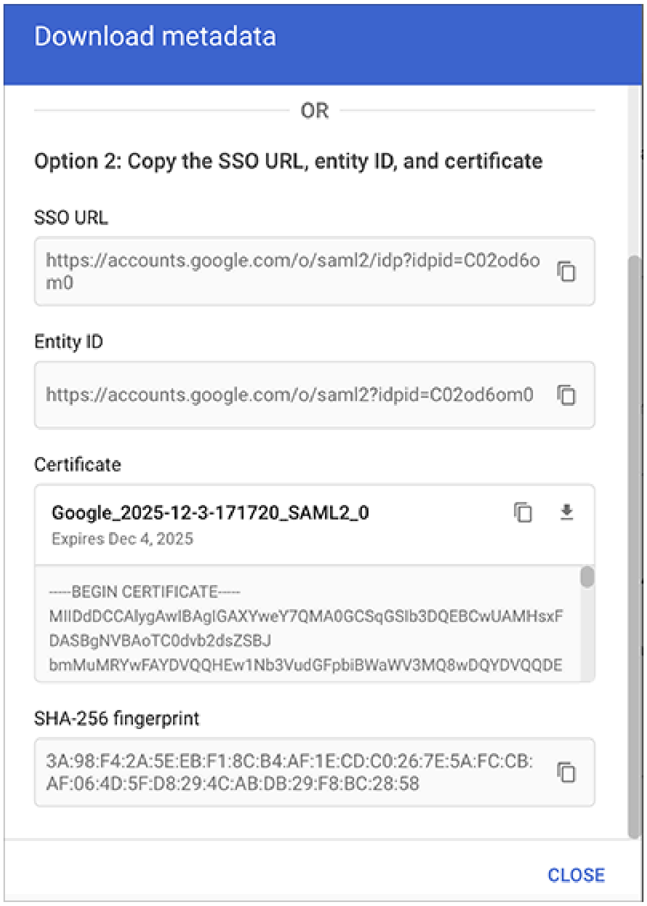
Employee Details > Title	→	jobTitle
Employee Details > Department	→	department

NOTE: *When the IdP includes `job title` and `department` in the SAML response, SOE automatically updates these user data fields on login. Including these attributes also allows you to use SOE's Connectivity reporting.*

Configure authentication settings in SOE

Next, you'll copy the configuration values from your new Google SAML application into SOE.

1. In Google, click **DOWNLOAD METADATA** to retrieve configuration values. You don't need to download the file. Instead, you'll copy and paste the information into SOE.



Download metadata

OR

Option 2: Copy the SSO URL, entity ID, and certificate

SSO URL

https://accounts.google.com/o/saml2/idp?idpid=C02od6om0

Entity ID

https://accounts.google.com/o/saml2?idpid=C02od6om0

Certificate

Google_2025-12-3-171720_SAML2_0

Expires Dec 4, 2025

```
-----BEGIN CERTIFICATE-----
MIIDdDCCAlygAwIBAgIGAXYweY7QMA0GCSqGSIb3DQEBCwUAMHsxF
DASBgNVBAoTC0dvb2dsZSBJ
bmMuMRYwFAYDVQQHEw1Nb3VudGFpbiBWaWV3MQ8wDQYDVQQDE
```

SHA-256 fingerprint

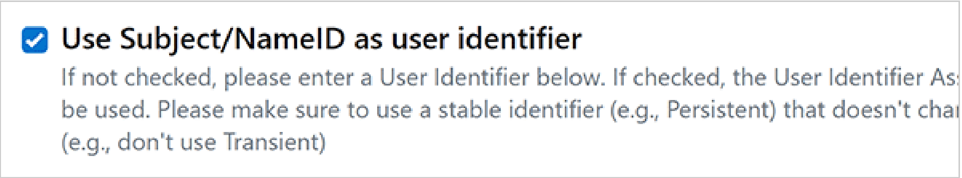
3A:98:F4:2A:5E:EB:F1:8C:B4:AF:1E:CD:C0:26:7E:5A:FC:CB:AF:06:4D:5F:D8:29:4C:AB:DB:29:F8:BC:28:58

2. In your SOE authentication settings, enter the following fields:
   - **Single Sign-On service URL** This is the **SSO URL** from the Google metadata box.
   - **Assertion consumer service URL** Set this to https://[your_site]/auth/saml2/post.
   - **Single Sign-On service protocol binding** Leave this set to **POST**.
   - **Issuer** This is the **Entity ID** you created in the "Configure the SAML Application" step above.
   - **Audience Restriction** Set this to the same value as **Issuer**.

   NOTE: *You won't use the **Entity ID** value from the Google metadata box. Instead, use the **Entity ID** you created in the "Configure the SAML Application" step (for example: StackOverflow).*

3. Copy and paste the following values from the Google SAML "Attribute Mappings" tab and metadata box into the corresponding SOE fields:
   - **Display Name Assertion** Set this to the Google app attribute you specified for display name (for example: displayName).
   - **Email Address Assertion** Set this to the Google app attribute you specified for email (for example: userEmail).
   - **Job Title** (optional) Set this to the Google app attribute you specified for job title (for example: jobTitle).
   - **Department** (optional) Set this to the Google app attribute you specified for department (for example: department).
   - **Identity Provider Certificates** Enter the full **Certificate** value from the Google metadata box (including the "BEGIN CERTIFICATE" and "END CERTIFICATE" lines).

4. **Use Subject/NameID as user identifier** is checked by default, which allows the IdP to specify the user identifier based on your SAML app configuration. This is the recommended setting.

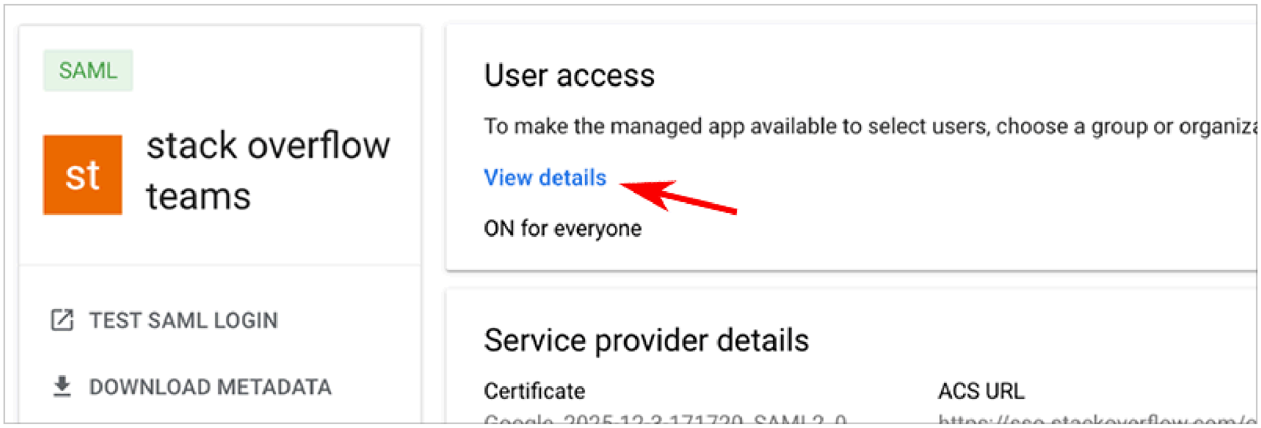


☑ Use Subject/NameID as user identifier

If not checked, please enter a User Identifier below. If checked, the User Identifier As be used. Please make sure to use a stable identifier (e.g., Persistent) that doesn't cha (e.g., don't use Transient)

If you uncheck this option, you can manually specify a **User identifier assertion** of your choice. Be sure to choose a user identifier that will never change (for example: login or user ID). Email address is *not* a good choice for user identifier, as email addresses can change.

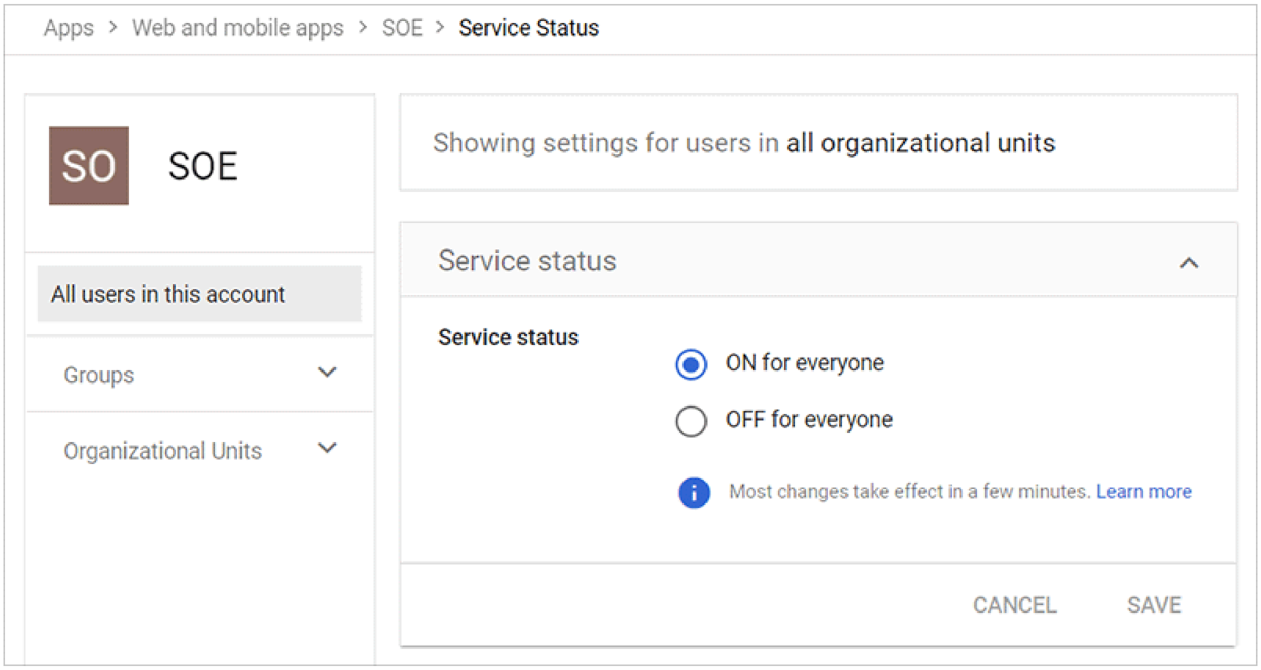
5. Only users (or user groups) assigned to your Google SAML app will be able to use SSO to log in to your SOE site. You can specify these users or groups in the "User access" section of your SAML app settings by clicking **View details**.



To make the managed app available to select users, choose a group or organiza

ON for everyone

You can also make your SAML application available to everyone within your Google workspace by setting **Service status** to **ON for everyone**.



Apps > Web and mobile apps > SOE > Service Status

SO SOE

Showing settings for users in all organizational units

Service status

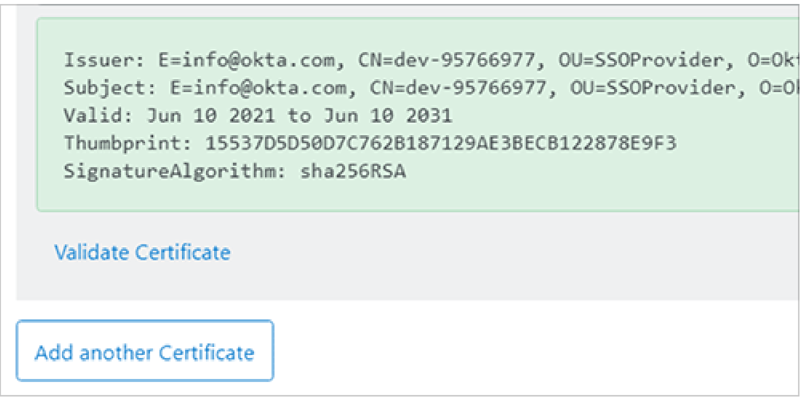
Service status

● ON for everyone

○ OFF for everyone

Most changes take effect in a few minutes. Learn more

6. Validate your certificate by clicking **Validate Certificate**. You should see a green box with a success message. If you don't, make sure you copied and pasted the full text of the certificate.

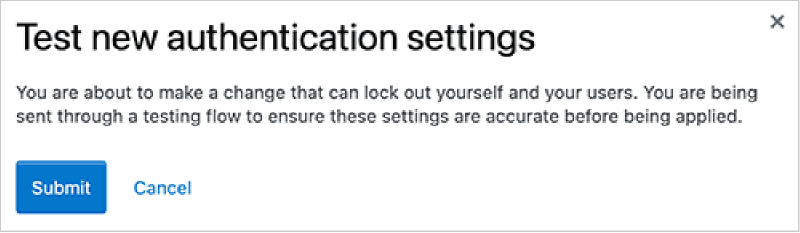


```
Issuer: E=info@okta.com, CN=dev-95766977, OU=SSOProvider, O=Ok
Subject: E=info@okta.com, CN=dev-95766977, OU=SSOProvider, O=O
Valid: Jun 10 2021 to Jun 10 2031
Thumbprint: 15537D5D50D7C762B187129AE3BECB122878E9F3
SignatureAlgorithm: sha256RSA
```

Test and save your SAML configuration

To complete the SSO setup, click **Save Settings**.

When saving settings, SOE will first perform an authentication test. If the test succeeds, SOE will apply your new authentication settings. Logged-in users stay logged in, as all active user sessions remain valid.



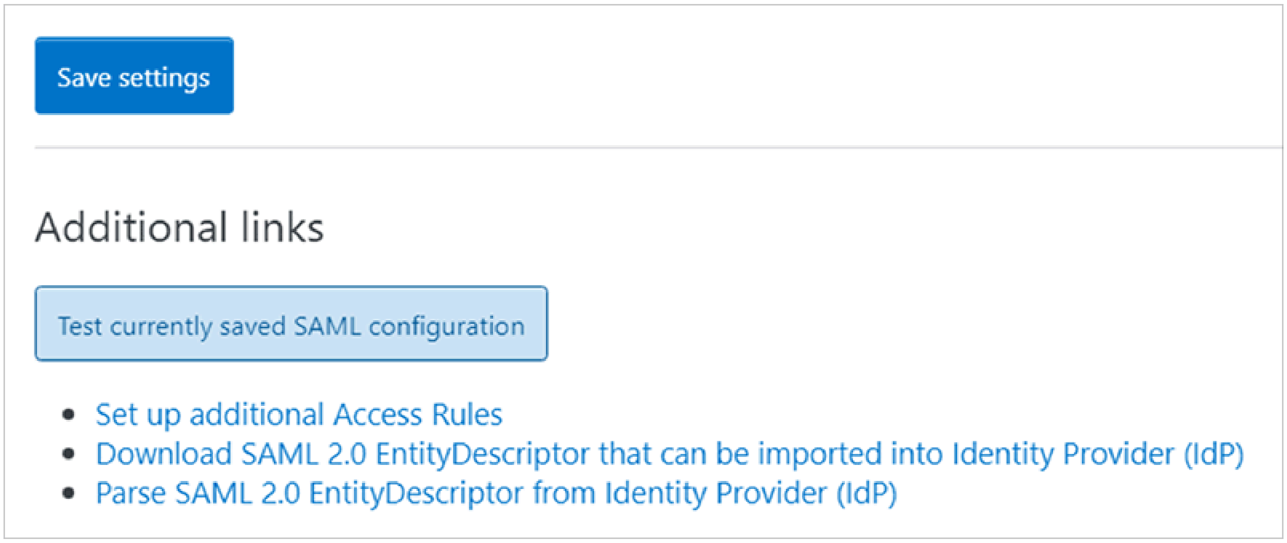
Test new authentication settings

You are about to make a change that can lock out yourself and your users. You are being sent through a testing flow to ensure these settings are accurate before being applied.

If the test fails, SOE will not apply the authentication settings. You'll stay on the SAML settings page so you can troubleshoot and correct problems.

This test acts as a safety net to keep invalid authentication settings from locking users (yourself included) out of your site. If you do find your users locked out of your site, reach out to Stack Overflow product support for help.

You can also click **Test currently saved SAML configuration** to display technical details about your SAML authentication. You'll find these helpful for understanding what information your IdP and SOE exchange. This is also useful when troubleshooting.


Save settings
Additional links
Test currently saved SAML configuration
Set up additional Access Rules
Download SAML 2.0 EntityDescriptor that can be imported into Identity Provider (IdP)
Parse SAML 2.0 EntityDescriptor from Identity Provider (IdP)

If you can't resolve the authentication errors, reach out to Stack Overflow support for help.

Maintain SAML certificates

You should rotate (replace) your Google SAML certificate well before its expiration date, or if it becomes compromised. If you don't replace a certificate before it expires, users won't be able to use SSO to sign in to any SAML applications that use that expired certificate.

For more information about maintaining SAML certificates, check out this helpful Google guide.