

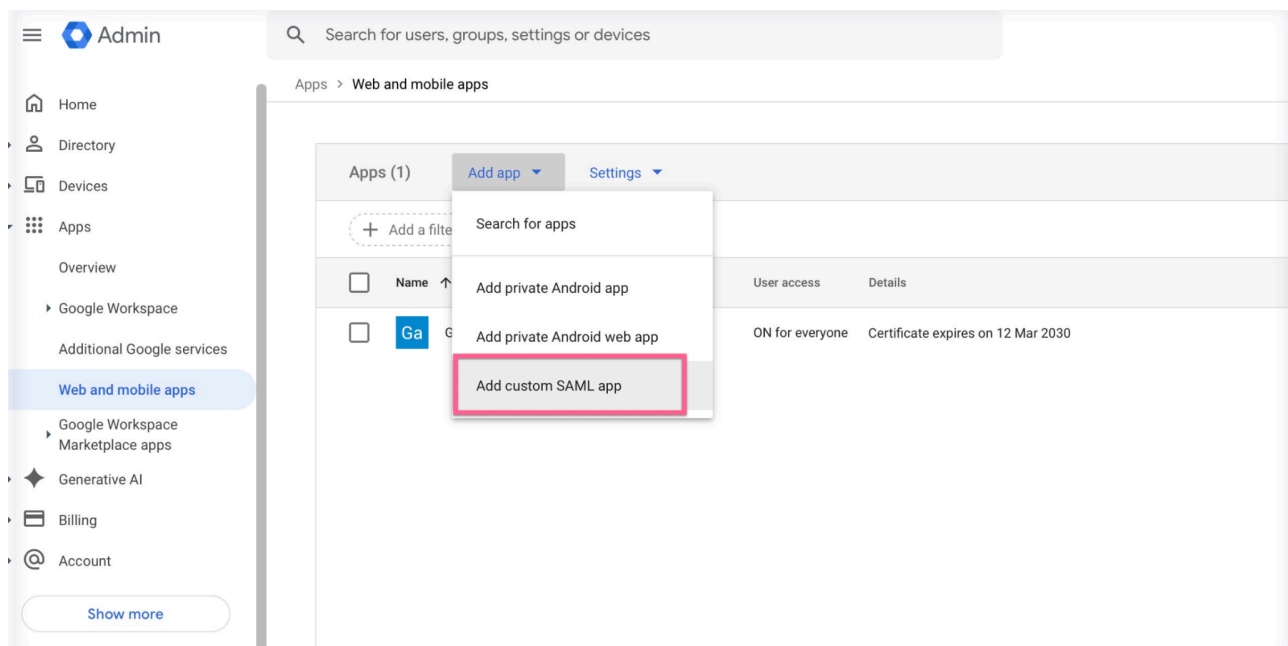
# Google Workspace SAML SSO Setup for Gainsight

---

## 1. Create a new custom SAML app in Google

Follow these steps in your Google Admin Console to begin setting up a new custom SAML application:

1. Go to the **Google Admin Console** (admin.google.com).
2. Navigate to **Apps** -> **Web and mobile apps**.
3. Click the **Add App** button.
4. Select **Add custom SAML app**.



To successfully set up a new custom SAML application in Google Workspace, you will complete the following four configuration steps:

1. **App Details:** Define the application's name, description, and icon.
2. **Google Identity Provider (IdP) Details:** Download the necessary metadata or certificate from Google to configure the Service Provider (SP).
3. **Service Provider (SP) Details:** Enter the application's specific ACS URL and Entity ID into the Google configuration.
4. **Attribute Mapping:** Define which user attributes (e.g., email, name) will be sent from Google to the application.

× Add custom SAML app

✓ App details — ✓ Google Identity Provider detail: — ✓ Service provider details — 4 Attribute mapping

Please note the following sequence for completing the 4 steps:

1. Complete the first two steps.
2. Log in to Gainsight and create the necessary authentication.
3. Complete the final two steps.

## App details

Define the application's name, description, and icon. Ex: GainsightSSO

×

Add custom SAML app

1 App details

2 Google Identity Provider detail

3 Service provider details

4 Attribute mapping

App details

Enter details for your custom SAML app. This information is shared with app users. [Learn more](#)

App name

App name is required

Description

App icon

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

CANCEL

CONTINUE

## Google Identity Provider (IdP) details

In the Google Identity Provider (IdP) details section, you have two methods for obtaining the necessary configuration information:

- **Option 1: Download IdP Metadata**
- **Option 2: Copy Individual Details**
  - You must manually copy the following three values:
    - Single Sign-On (SSO) URL
    - Entity ID
    - Certificate

×

Add custom SAML app

✓ App details

2 Google Identity Provider details

3 Service provider details

4 Attribute mapping

To configure Single Sign-On (SSO) for SAML apps, follow your service provider's instructions [Learn more](#)

Option 1: Download IdP metadata

DOWNLOAD METADATA

OR

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

SSO URL

Entity ID

Certificate

To set up the Google IdP for Gainsight, you must use **Option 2: Copy the SSO URL, entity ID, and certificate**. Please **copy the SSO URL and the Entity ID**, and **download the Certificate**.

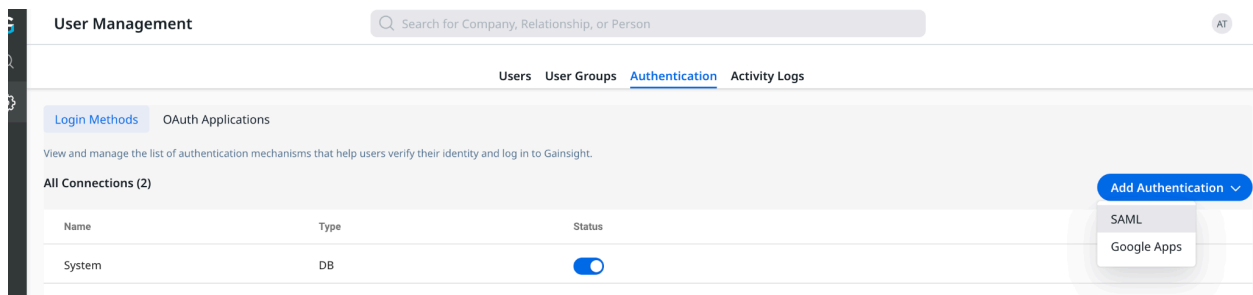
## 2. Create the SAML Authentication in Gainsight

### 1. Navigate to Gainsight Administration

Go to **Administration > User Management > Authentication**.

### 2. Add SAML Authentication

Click **Add Authentication** and select **SAML**.



## Authentication details

Please enter the following details to create the authentication record:

- **Name:** Provide a name for the application.  
(E.g., *GoogleSSO*)
- **Email Domain:** Enter your organization's domain.
- **Sign In URL:** Paste the **SSO URL** copied from the Google IdP.
- **Certificate:** Upload the **Certificate** downloaded from the Google IdP.

Now **SAVE** the connection

The screenshot shows the 'SAML Mechanism' configuration form. It includes fields for 'Name' (with a placeholder 'GoogleIDP'), 'Email Domain', 'Sign In URL', and 'Sign Out URL'. There's a 'Certificate' section with a file upload icon and a filename 'Google\_2030-3-12-01353\_SAML2\_0.pem'. At the bottom, there's a 'Field Mapping' section with 'Source Field' and 'Target Field' both set to 'Username'. The form has 'Cancel' and 'Save' buttons at the bottom right.

### 3. Download Gainsight metadata XML

Now, when you **edit the same connection**, you will see a **Download** option to retrieve an XML file as shown below

**SAML Mechanism**

Name \*

GoogleIDP

Enter a unique connection name for authentication

Email Domain \*

Enter the domain name for SAML authentication

Sign In URL \*

Enter SAML login URL for authentication

Sign Out URL

Enter Sign Out URL

Enter SAML logout URL to exit from authentication

Certificate \*

Drag and drop file here or Browse

Field Mapping

Source Field

Username

Target Field

Username

Enter the name of the claim containing User attributes from the source to be mapped to the Username

Download

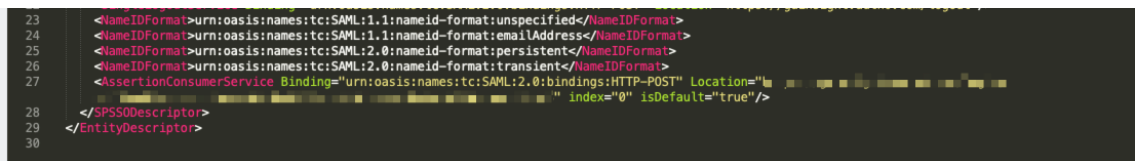
Cancel

Save

## 4. Extract ACS URL and Entity ID from the XML

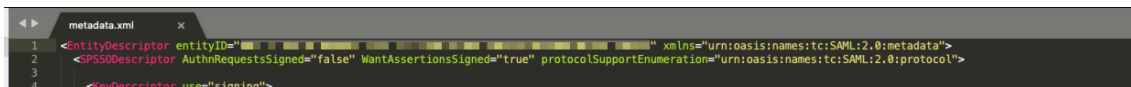
To complete the setup, you need to open the downloaded XML file and copy the following two values:

- **AssertionConsumerService → Location.** Towards the bottom of the file. It would be the blurred-out section from the image below. This would need to be copied.



```
23 <NameIDFormat>urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified</NameIDFormat>
24 <NameIDFormat>urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress</NameIDFormat>
25 <NameIDFormat>urn:oasis:names:tc:SAML:2.0:nameid-format:persistent</NameIDFormat>
26 <NameIDFormat>urn:oasis:names:tc:SAML:2.0:nameid-format:transient</NameIDFormat>
27 <AssertionConsumerService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST" Location="
28 </SPSSODescriptor>
29 </EntityDescriptor>
30
```

- **Entity ID.** Towards the top of the file, it would be the blurred-out section from the below image. This would need to be copied.



```
1 <EntityDescriptor entityID="
2 <SPSSODescriptor AuthnRequestsSigned="false" WantAssertionsSigned="true" protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol">
3
4 <KeyDescriptor use="signing">
```

## 5. Finish app details in Google

### Service Provider details

Now, navigate to the **Service Provider Details** section within your Google App settings.

Enter the following information that you extracted from the downloaded XML file:

- **ACS URL:** Paste the value you copied from the **AssertionConsumerService -> Location** attribute in the XML file.
- **Entity ID:** Paste the **Entity ID** value you copied from the XML file.

Then Click CONTINUE

The screenshot shows the 'Add custom SAML app' configuration page in Google Admin. The page has a blue header with a close button and the title 'Add custom SAML app'. Below the header is a progress bar with four steps: 'App details' (checked), 'Google Identity Provider detail' (checked), 'Service provider details' (active), and 'Attribute mapping' (disabled). The main content area is titled 'Service provider details' and includes a subtitle: 'To configure Single Sign-On, add service provider details such as ACS URL and entity ID. [Learn more](#)'. There are three input fields: 'ACS URL' (containing a long alphanumeric string), 'Entity ID' (containing a long alphanumeric string), and 'Start URL (optional)'. Below the 'Start URL' field is a checkbox labeled 'Signed response'. Further down is a section for 'Name ID' with a subtitle: 'Defines the naming format supported by the identity provider. [Learn more](#)'. This section includes a 'Name ID format' dropdown menu set to 'UNSPECIFIED' and a 'Name ID' dropdown menu set to 'Basic Information > Primary email'.



# Attribute mapping

Map the attributes as follows:

- Map the **Primary Email** attribute to **Username**.

Click **FINISH** to complete the configuration.

×

Add custom SAML app

✓ App details

✓ Google Identity Provider detail:

✓ Service provider details

4 Attribute mapping

Attributes

Add and select user fields in the Google Directory, then map them to service provider attributes. Attributes marked with \* are mandatory. [Learn more](#)

Google directory attributes

Basic Information >

Primary email

→

App attributes

Username

×

ADD MAPPING

Group membership (optional)

Group membership information can be sent in the SAML response if the user belongs to any of the groups that you add here.

Google Groups

Search for a group

→

App attribute

Groups

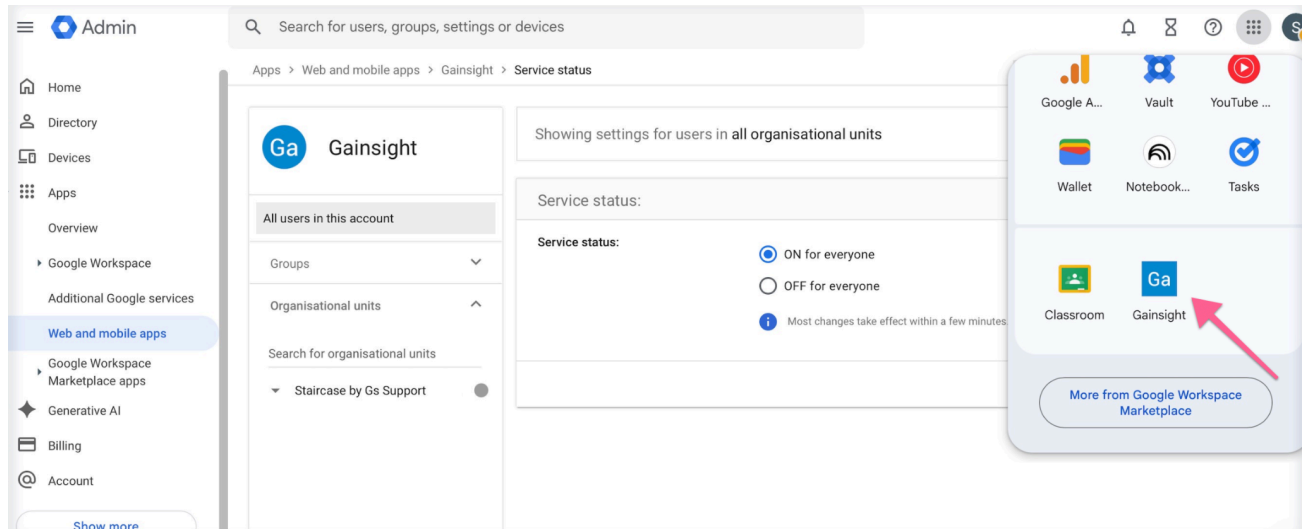
BACK

CANCEL

FINISH

## 6. Assign users/groups to the SAML app

Now that the application setup is complete, you must **assign users to a group** to grant them access to the application.



## 7. Test SAML and then disable DB Authentication

- **Test SAML login:**
  - Use a test user who has the app assigned.
  - Confirm they can access Gainsight successfully.
- **Roll out to admins and end users** as needed.
- Once you're confident SAML is working for all required users, **raise another ticket with Gainsight Support** to:
  - **Disable temporary DB Authentication** for your org and/or specific users.