

Configuring SSO with G Suite

Last Modified on Nov 4, 2020

This article provides a step-by-step guide to configuring SSO between OnceHub and G Suite.

Requirements

To configure SSO in your account, you must be a OnceHub Administrator. However, you do not need a product license. [Learn more](#)

You must already have an account with G Suite. The person configuring in G Suite must be an administrator with access to the admin portal.

Step-by-step directions

Request access

SSO is intended for accounts with multiple users who take the extra security measure of signing into third-party applications using an identity provider. Please [contact us](#) to learn more. OnceHub can enable the SSO functionality in your account manually.

SAML configuration

You can access SAML configuration at OnceHub **Account settings** -> In the lefthand sidebar, select **Security** -> **SSO**.

OnceHub provides specific field values you can copy and configure within G Suite.

1. Create a new SAML app

In G Suite, go to **Apps** -> **SAML apps**.

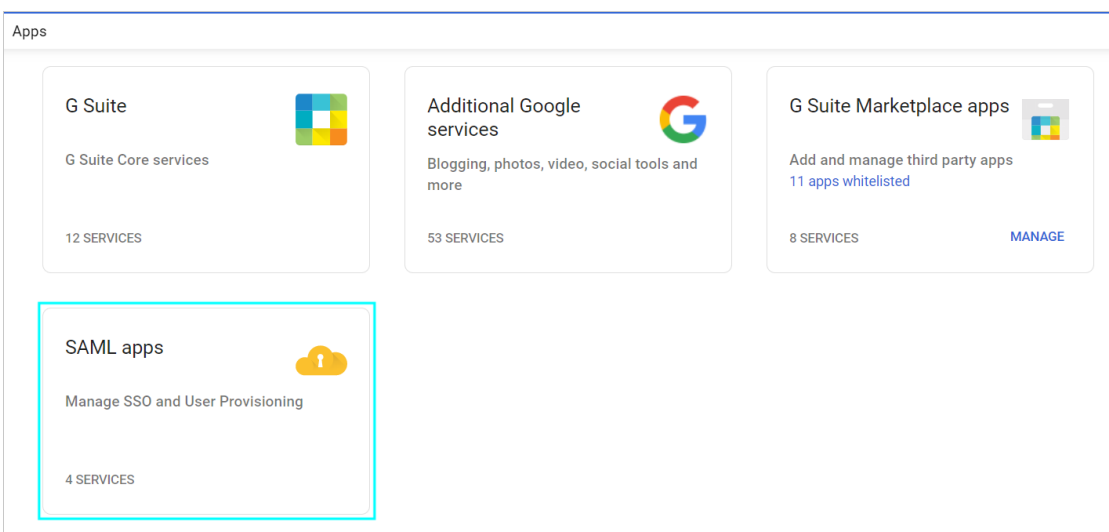


Figure 1: Create new SAML app

On the bottom right, click the **Add +** icon. In the popup, select **Setup my own custom app**.

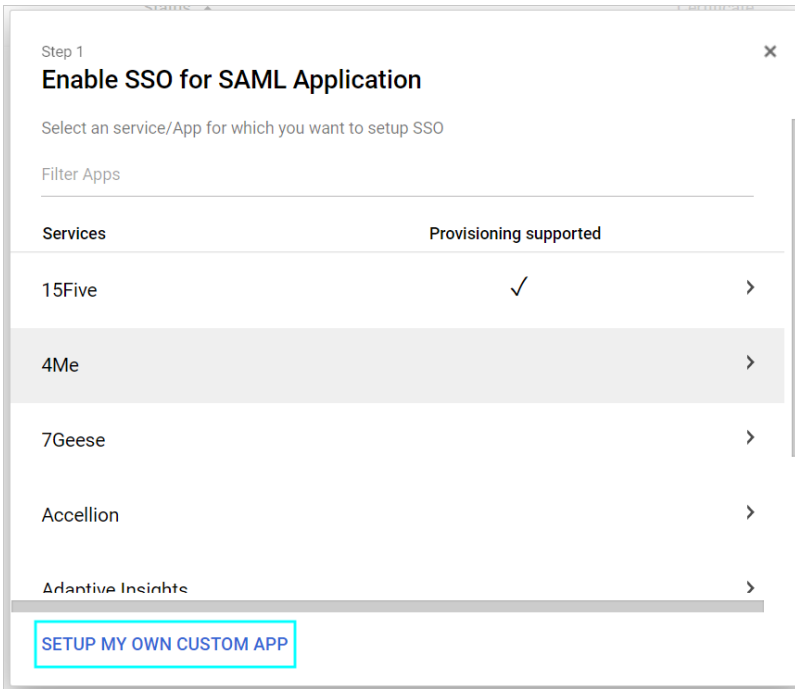


Figure 2: Setup my own custom app

2. Grab information from G Suite

On the **Google IdP Information** step, copy the SSO URL and Entity ID. Paste them into a text document so you can come back to them.

Next, download the **Certificate**. Set these aside for a moment and select **Next** in G Suite.

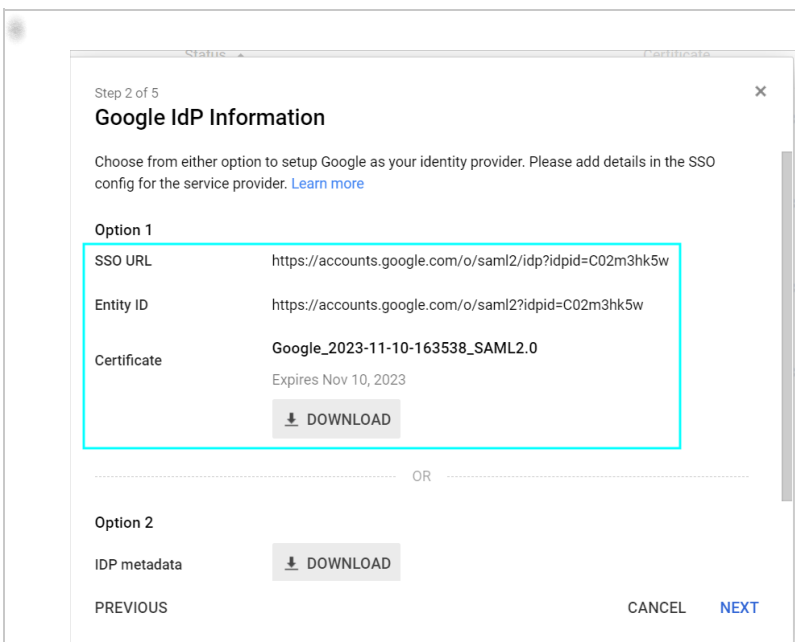


Figure 3: Google IdP Information

3. Basic information

In the **Basic information for your Custom App** step, give the app a name (for instance, OnceHub). When you're

satisfied with the basic information, select **Next**.

Figure 3: General Settings

3. Service Provider Details from OnceHub

On the **Service Provider Details** step, fill out the settings. You can grab these values in OnceHub, on the **Required by identity provider** step.

Figure 4: Configure SAML Settings

In G Suite	In OnceHub
Entity ID	Identifier URL

ACS URL

ACS URL

[Not required; G Suite refers to ACS URL for this function]

Single sign-on URL

4. Attribute mapping

For the **Name ID** field on the same step as above, select **Basic information** and then **Primary Email** (Figure 4).

You can keep the **Name ID Format** on **UNSPECIFIED**.

Once you're ready, click on **Next**. The Attribute Mapping step will display the **Primary Email** field. Add a mapping that maps this to the application attribute **email** (all lower case).

Select **Finish**.

5. Paste G Suite information in OnceHub

Go back to OnceHub and refer to the saved information from the **Google IdP Information** step (step two above). Paste the relevant values in OnceHub

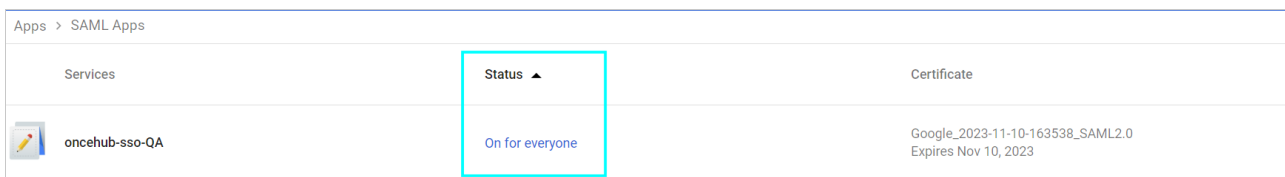
In G Suite	In OnceHub
Entity ID	Entity ID
SSO URL	IDP single sign-on URL
Certificate	Public x509 certificate

Important:

For the Public x509 certificate, include the **-----BEGIN CERTIFICATE-----** and **-----END CERTIFICATE-----** syntax in your selection and paste it all into the OnceHub field.

6. Status in G Suite

Before clicking Verify in OnceHub, go back to G Suite and access the **SAML apps** section again. Make sure the status of the new SAML app is on for all relevant users. This may be **On for everyone** or **On for some** (a specific group you define in G Suite).




Services	Status	Certificate
 oncehub-ss0-QA	On for everyone	Google_2023-11-10-163538_SAML2.0 Expires Nov 10, 2023

Figure 8: Assign to People

7. Verify

In OnceHub, click **Verify** to confirm that SAML authentication is verified.

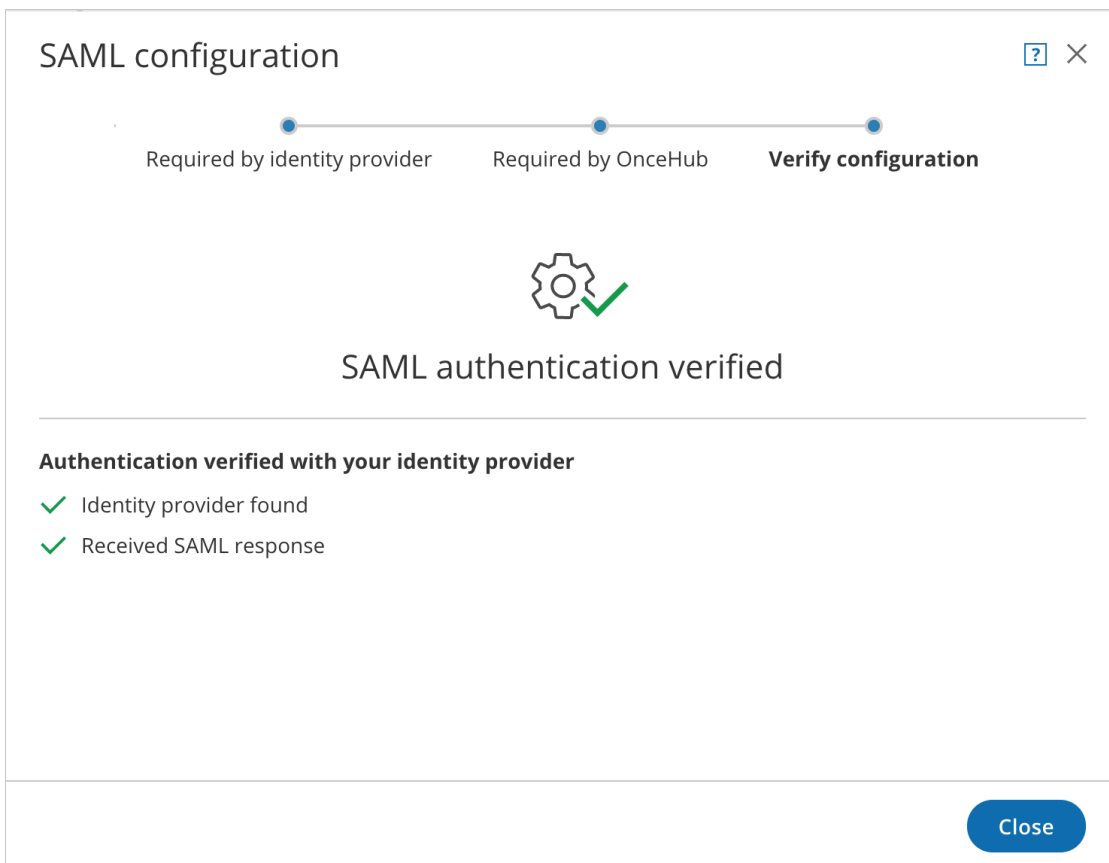


Figure 9: Verify configuration

8. Enable SSO for all users

Once you've verified your SSO configuration, you can select the **Enable SSO for all users** toggle. All Users in your OnceHub account can now [access their account using SSO](#).

Important:

Before you enable the account, make sure all your Users have matching email addresses for their OnceHub User profile and their G Suite profile.

Once SSO is enabled, they **will not** be able to change their OnceHub email.

If their OnceHub email does not match the email in their IDP profile, they **will not** be able to log in.

Security

SSO

SAML-based SSO allows your Users to sign into OnceHub using your organization's identity provider. [Learn more](#)

Setup SAML configuration for SSO Setup

Enable SSO for all users ON

i Once SSO is enabled, all users in your account will require to sign in with SSO and won't be able to sign in using password.

Figure 15: Enable SSO for all users

i Note:

If existing Users were already signing into OnceHub using an email and password, they will no longer be able to do so. They will only be able to sign in using SSO.