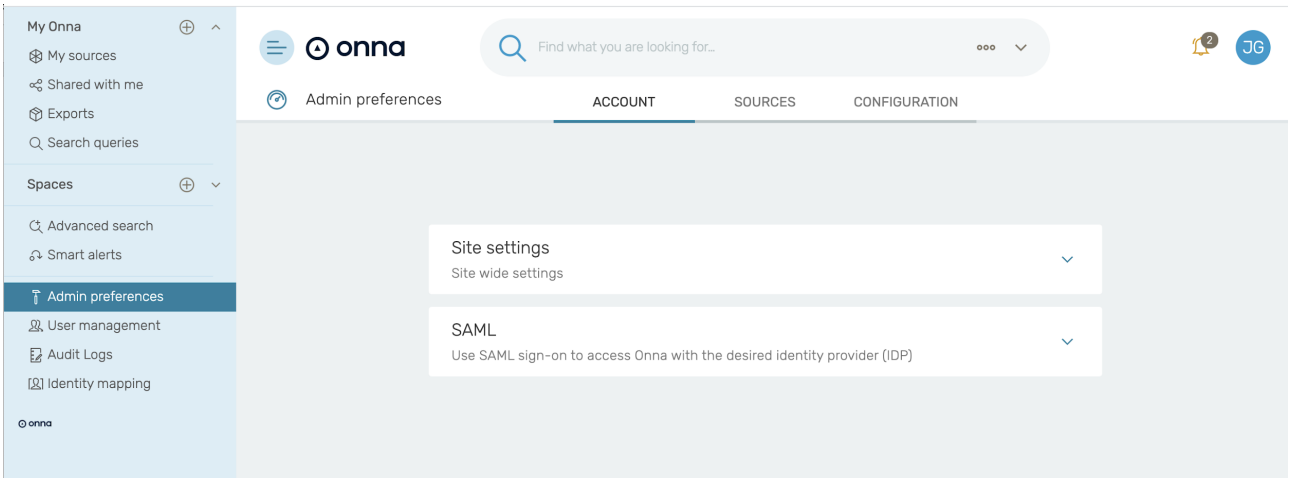
SAML 2.0 Integration

Onna offers Single Sign On (SSO) integration through SAML 2.0 (Secure Assertion Markup Language) with a variety of compliant identity providers allowing you to leverage your existing user base and authentication mechanism to use the platform. There are only a few steps required to configure your Identity Provider (IdP) using the Onna Admin dashboard.

This guide walks you through setting up Onna as a Service Provider (SP). You will fill-in information about your Identity Provider (IdP), the external 3rd party which your users will sign-in through, and will return credentials back to Onna in the form of a SAML assertion. On the other end, you will also need to configure your IdP to establish communication with the Onna SP. By default, provisioning is enabled for your account. The default role in Onna for users created by provisioning is ‘user’. In the event you wish to turn off provisioning for an account please contact the Onna Support Team. Once provisioning has been turned off, if a user has not been provisioned in Onna and attempts to use SSO identity to sign in, they will have no permissions until an Onna admin configures an Onna user for this identity.

To get started, open the **Admin Preferences** → **Account** → **SAML** with the proper administrator user:



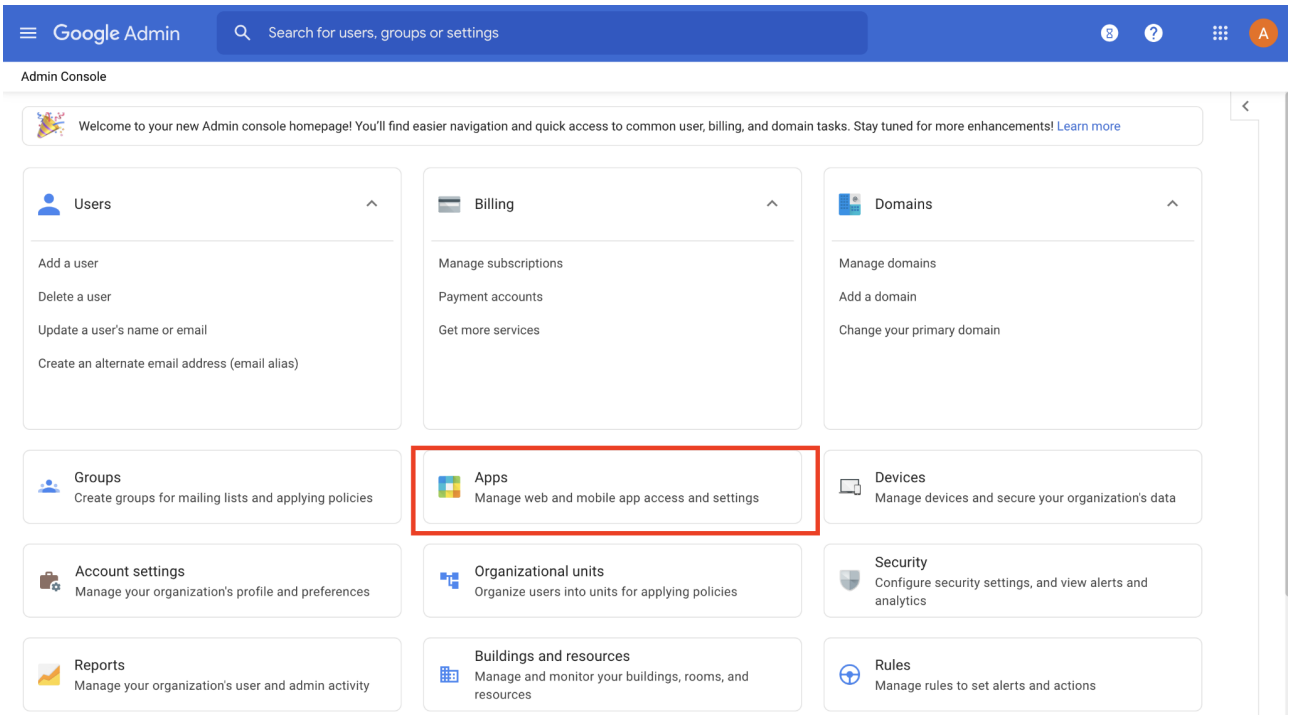
The following settings are configurable under the SAML section.

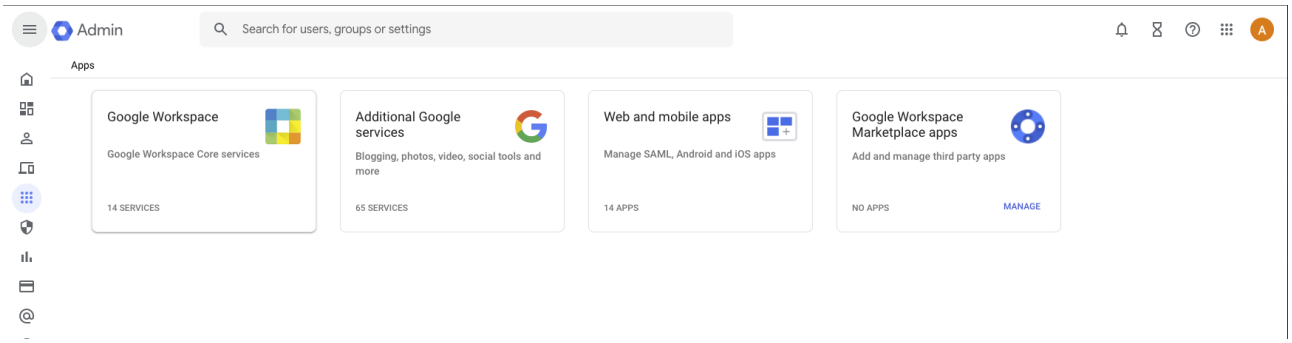
- **IdP ID / {IdPName}**: Choose any name that you prefer to identify this Identity Provider (IdP). We'll refer to this value as **{IdPName}** in the rest of the document.
    - This name will be displayed to the users in a selection box should you have more than one IdP. We suggest providing the ID in the following format:
        - youraccountname-identifyprovider
        - Example of how the IdP ID / IdPName should look: ***companyname-google***
- **IdP Issuer:** The identity provider's URL
- **SSO URL**: The single sign-on URL of the SAML Identity Provider Login page that your users will be redirected to for logging in.
- **Certificate**: The public x509 certificate of the SAML Identity Provider.

Setting up Google Workspace:

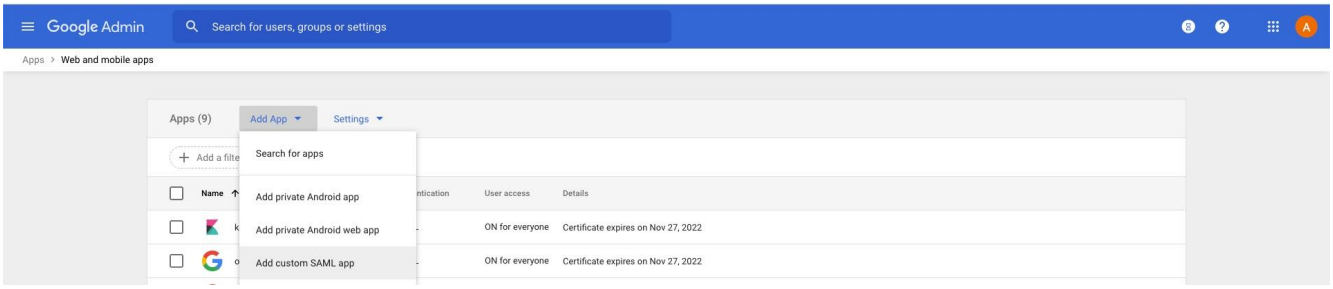
Here is a sample workflow using Google Workspace as an Identity Management tool.

1. To get started, log in to Google Workspace and navigate to the admin console. Click on **'Apps'** and select **'Web and mobile apps'.**

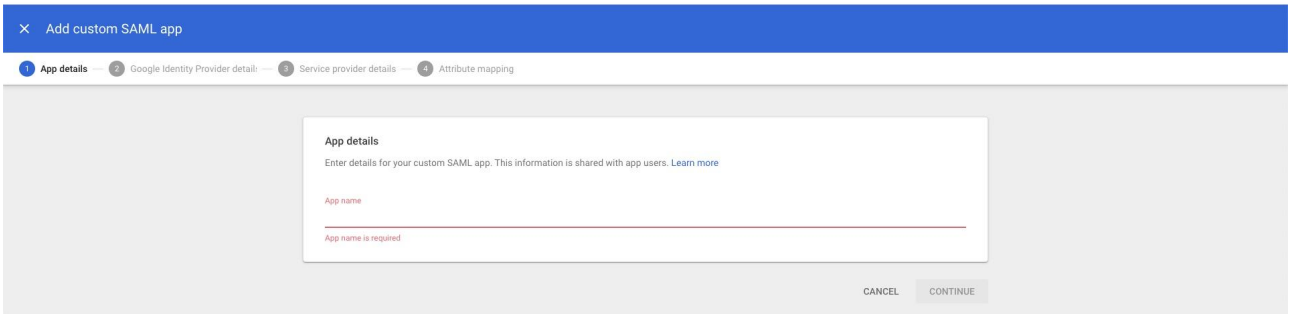




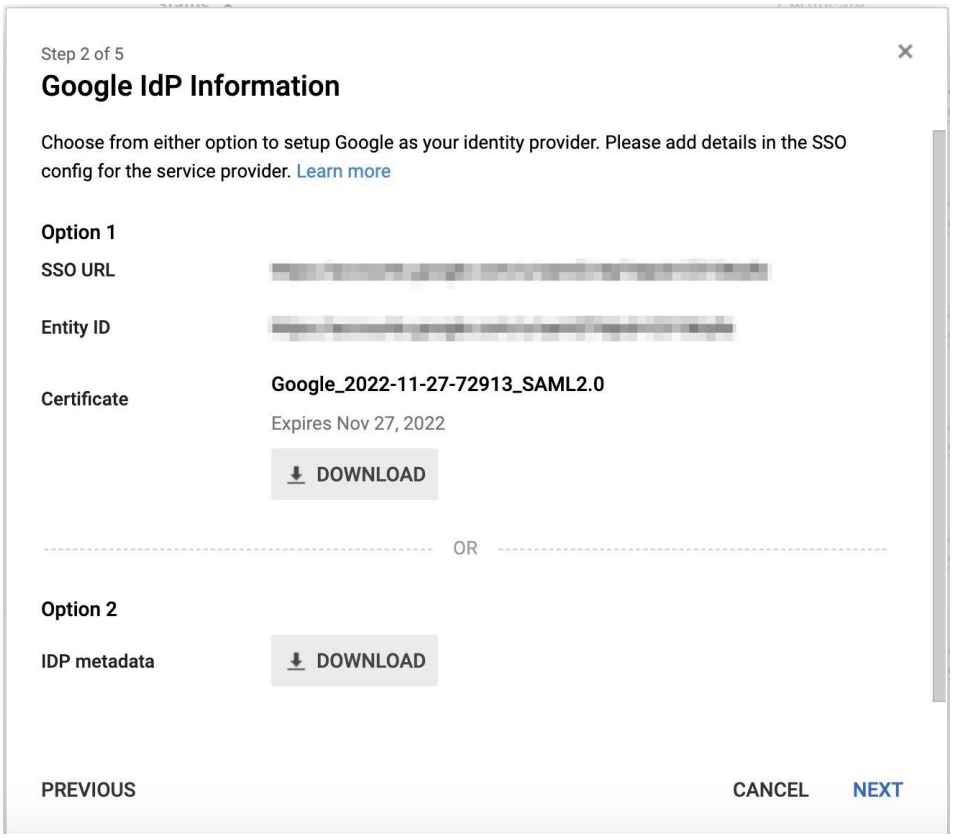
2. Click on **‘Add App’** at the top of the screen. From the dropdown select **‘Add custom SAML app’**



3. Provide a name for the new SAML app



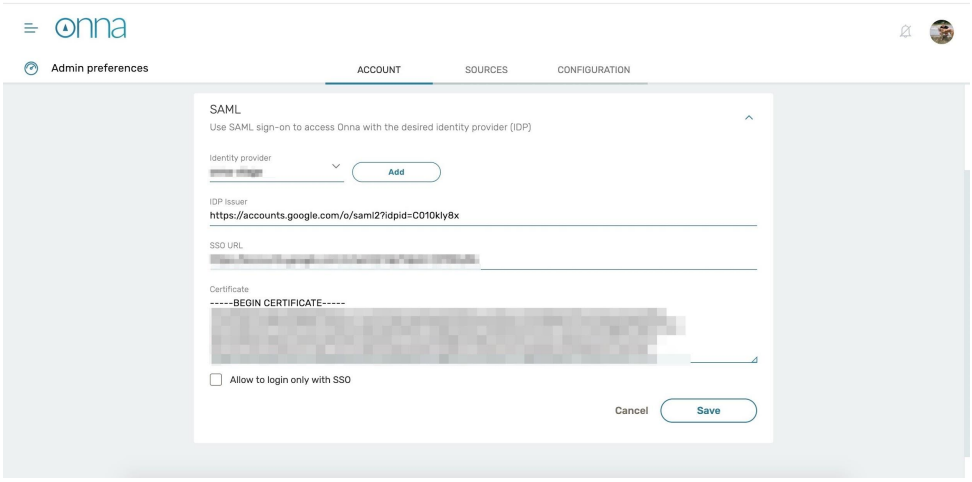
4. Use the values to complete the SSO setup in your Onna configuration



SSO URL will be used for the **SSO URL** field in Onna.

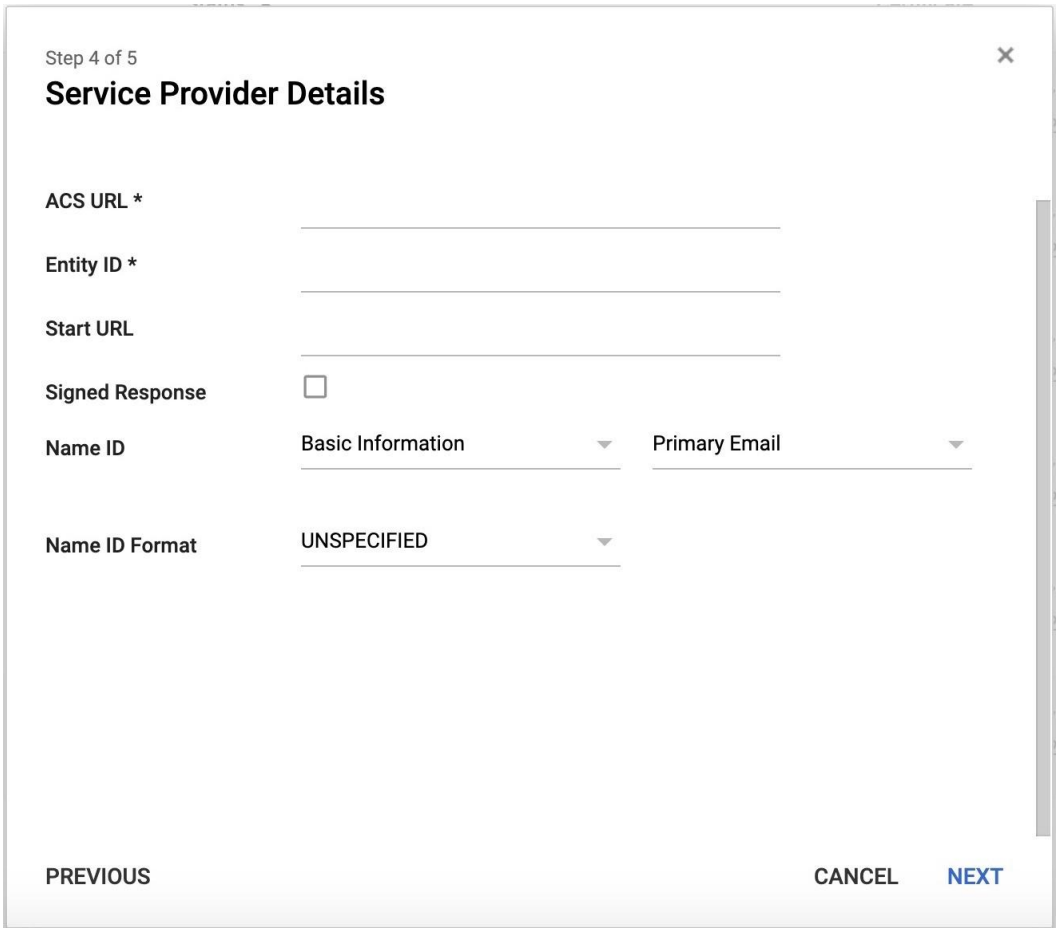
Entity ID will be used for the **IDP Issuer** field in Onna.

5. In Onna, the completed configuration:



Note: Do not enable 'Allow to login only with SSO' until you verify you are able to login via SSO

6. Within the recently created SAML app in Google Workspace, there are only a few items you need to fill in with the main ones shown below.

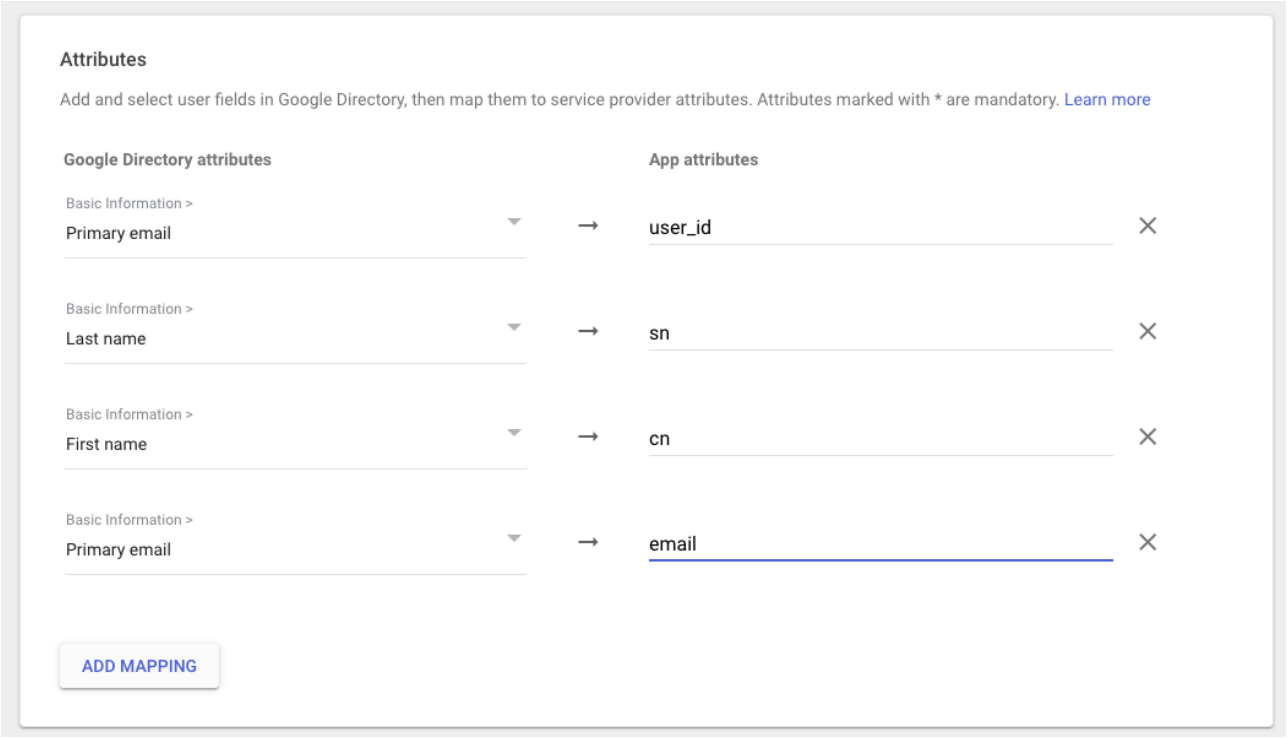


- **ACS URL:**
  - https://enterprise.onna.com/auth/oauth/saml/?acs
- **Entity ID:**
  https://enterprise.onna.com/auth/oauth/saml/metadata?idpId={IdPName}
  - **{IdPName}** needs to be replaced with the name you chose to identify your IdP (see page 2 for more information)
- **Start URL:**
- https://enterprise.onna.com/{youraccount}/signin?idpId={IdPName}&scopes={youraccount}
  - **{youraccount}** needs to be replaced by the account name in your Onna URL.

- **{IdPName}** needs to be replaced with the name you chose to identify your IdP (see page 2 for more information)

Note: Enable Signed Response

7. Once the above has been completed you can click 'NEXT'.



Only the **attributes** listed below are **required** to complete the SAML configuration with Onna.

- Primary email - **user_id**
- Last name - **sn**
- First Name - **cn**
- Primary email - **email**

8. After the attributes have been added you can click 'FINISH'. You can now enable the Service Status for everyone or for certain organizations.

Note - Changes may take up to 24 hours to propagate to all users.

Delete SAML and SSO:

1. You can delete your own SAML and SSO configuration in Onna from the Admin preferences.
2. To get started, open the Admin Preferences → Account → SAML with the proper administrator user.
3. Click on ‘Identity Provider’ and from the dropdown select the configuration you would like to remove.
4. At the bottom of the screen click ‘delete’ to permanently remove the SAML configuration in Onna.