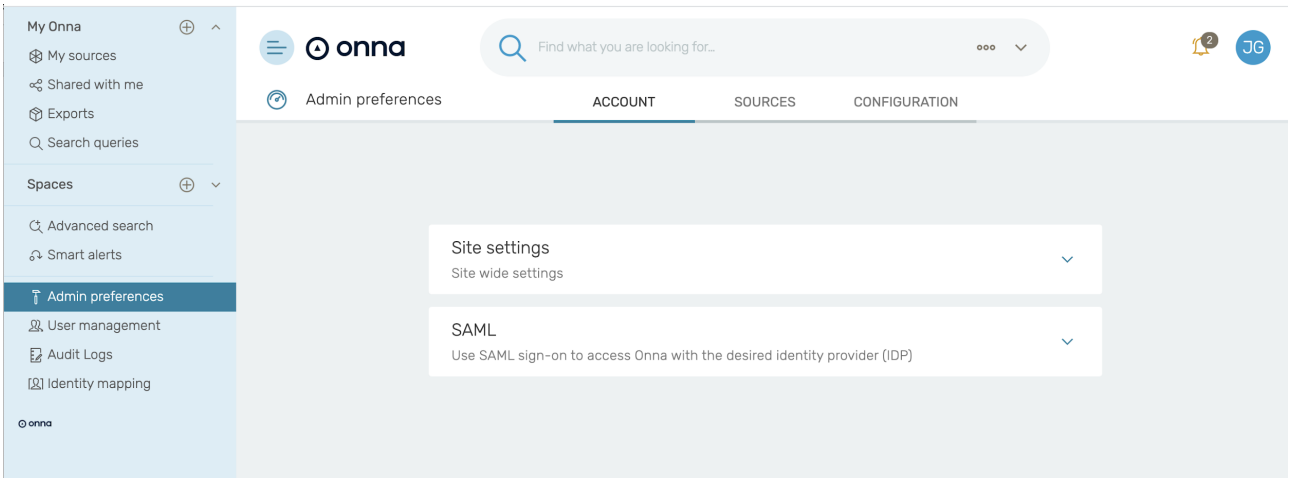
# SAML 2.0 Integration

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-okta***
- **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.

The next step is to configure your IdP so that it can establish communication with the Onna service provider. Below are the items that need to be configured. There are only a few items you need to fill in with the main ones shown below:

- **Onna Audience Restriction URL**:
  - 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)
- **Onna SAML Assertion Consumer Service:**
  - https://enterprise.onna.com/auth/oauth/saml/?acs
- **Name id format:**
  - The required nameid format is "urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress", so an email address is needed to identify the user in the system.
  - The email address must match exactly to the case for the user's authentication to work. If the user was created in Onna with an all lower case email, the id sent from your identity manager must also be lower case. In Okta, you can use this expression such as String.toLowerCase(user.email).

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

- **user_id :** email address
- **sn**: last name
- **cn**: first Name
- **email**: email address

**Enabling Sign in through IdP**

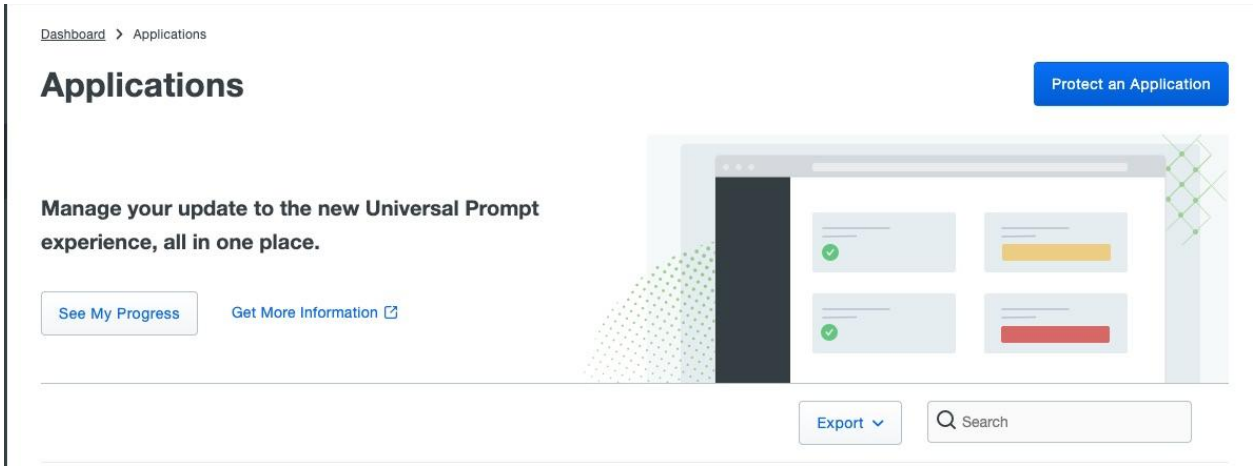
- In order to use an Okta 'chiclet' or similar solution, you must provide a value for Default Relay State.

- **Default Relay State:**
  - 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)

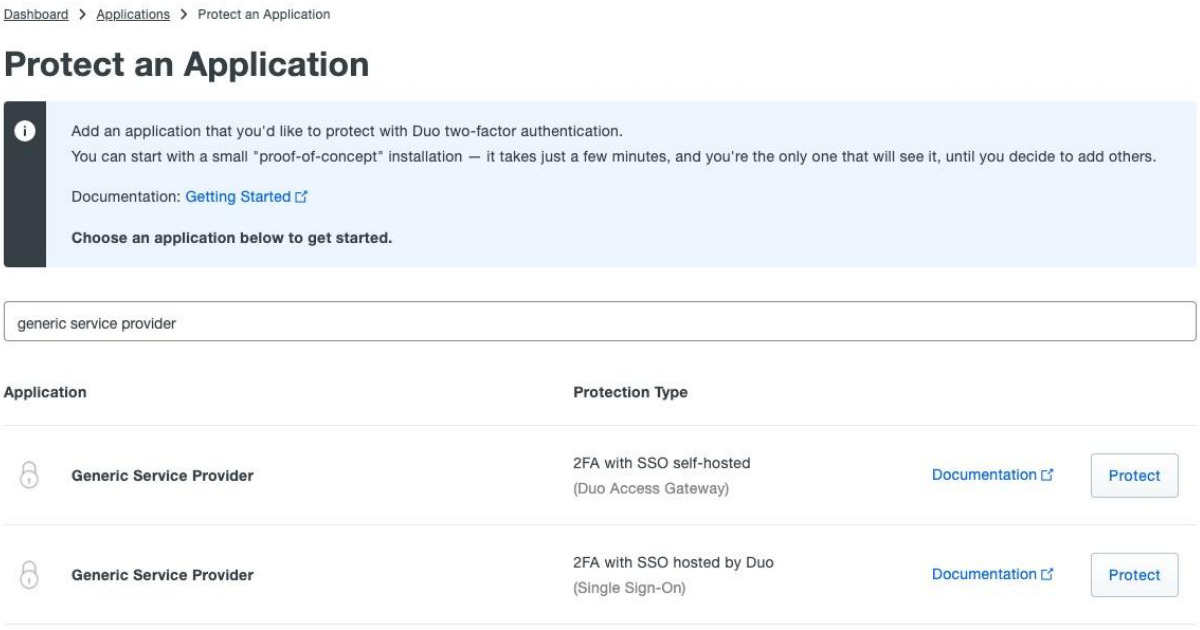
# Setting up Duo:

Here is a sample workflow using Duo as an Identity Management tool.
Before configuring your service provider application you'll first need to enable Duo Single Sign-On for your Duo account and configure a working authentication source.

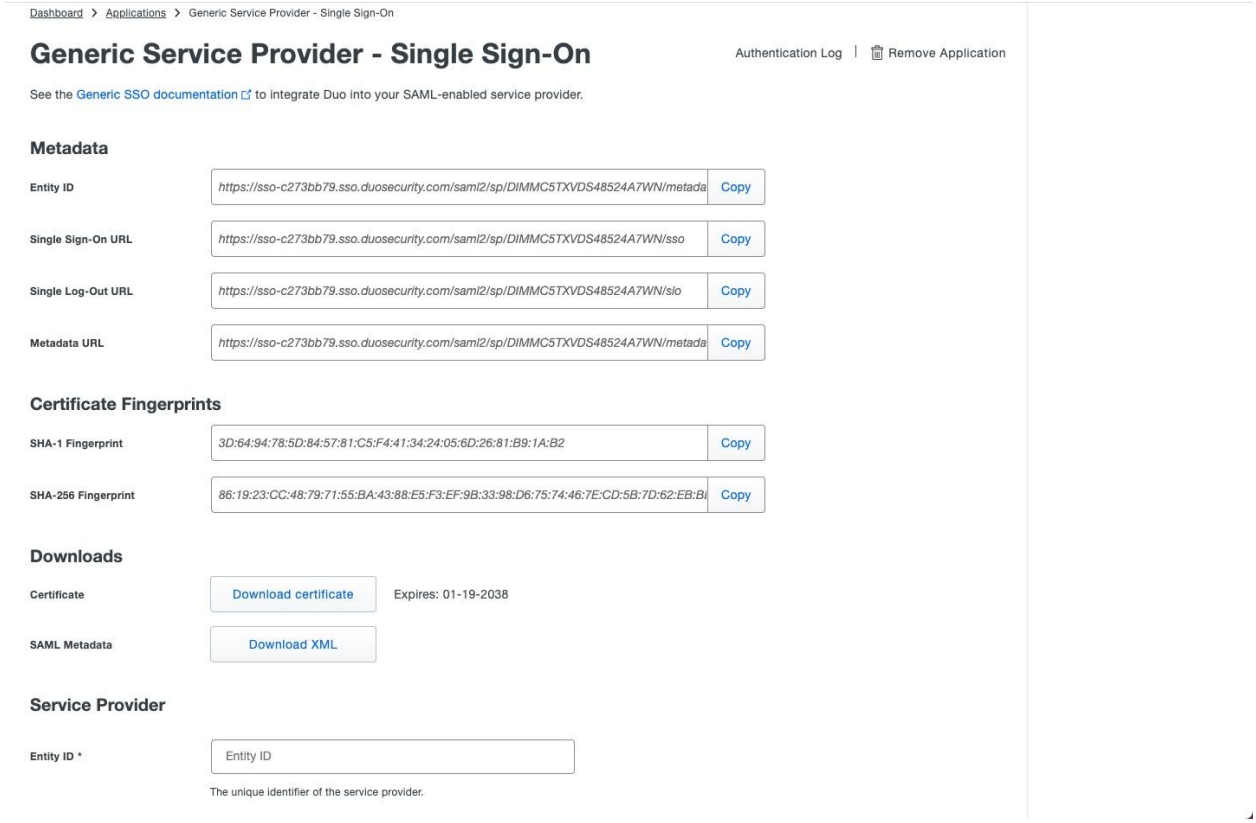
1) To get started, login to Duo and navigate to 'Applications'.
2) Click 'Protect an application' and search for 'Generic Service Provider'



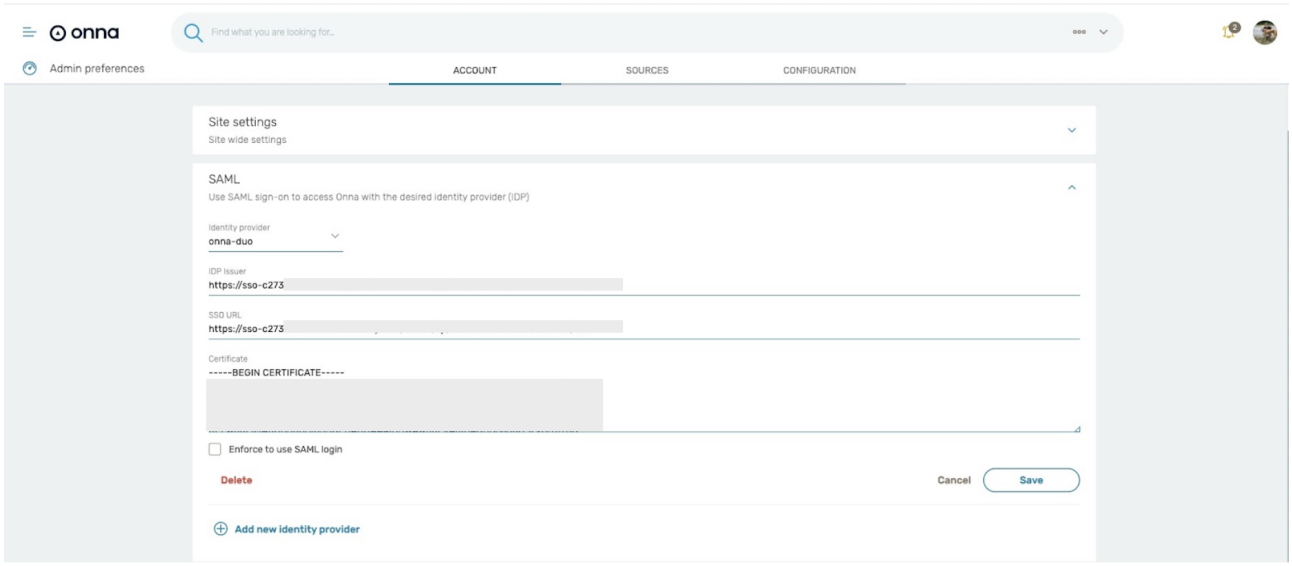

3) Select the application that shows the single sign on option




4) Use the values under metadata to complete the SSO setup in your Onna configuration

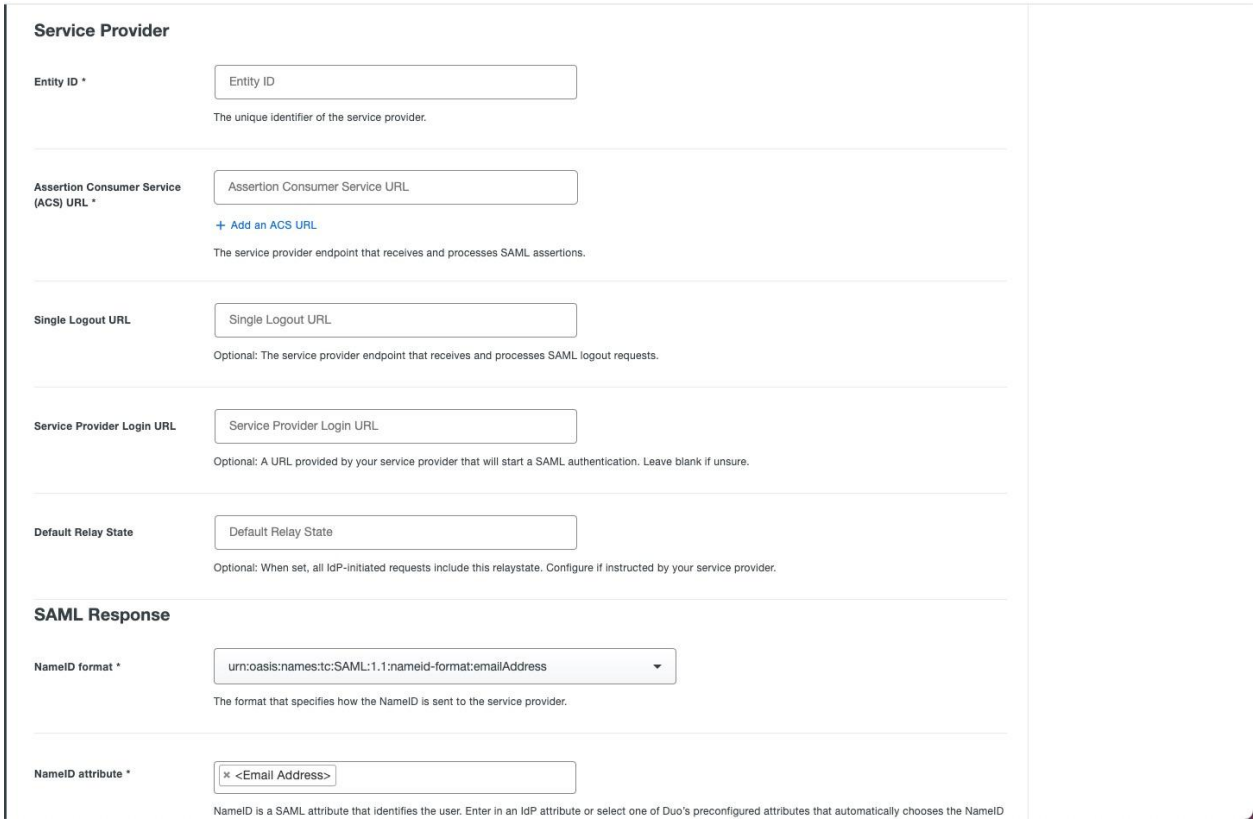



5) In Onna, the completed configuration:




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

6) Once the changes have been saved, navigate back to the Generic Service Provider in Duo & scroll down to the section 'Service Provider' .




There are only a few items you need to fill in with the main ones shown below. Please replace {IdPName} with the name of the Idp service you have configured in Onna:

**Entity ID**:
https://enterprise.onna.com/auth/oauth/saml/metadata?idpId={Name of your IdP in Onna}

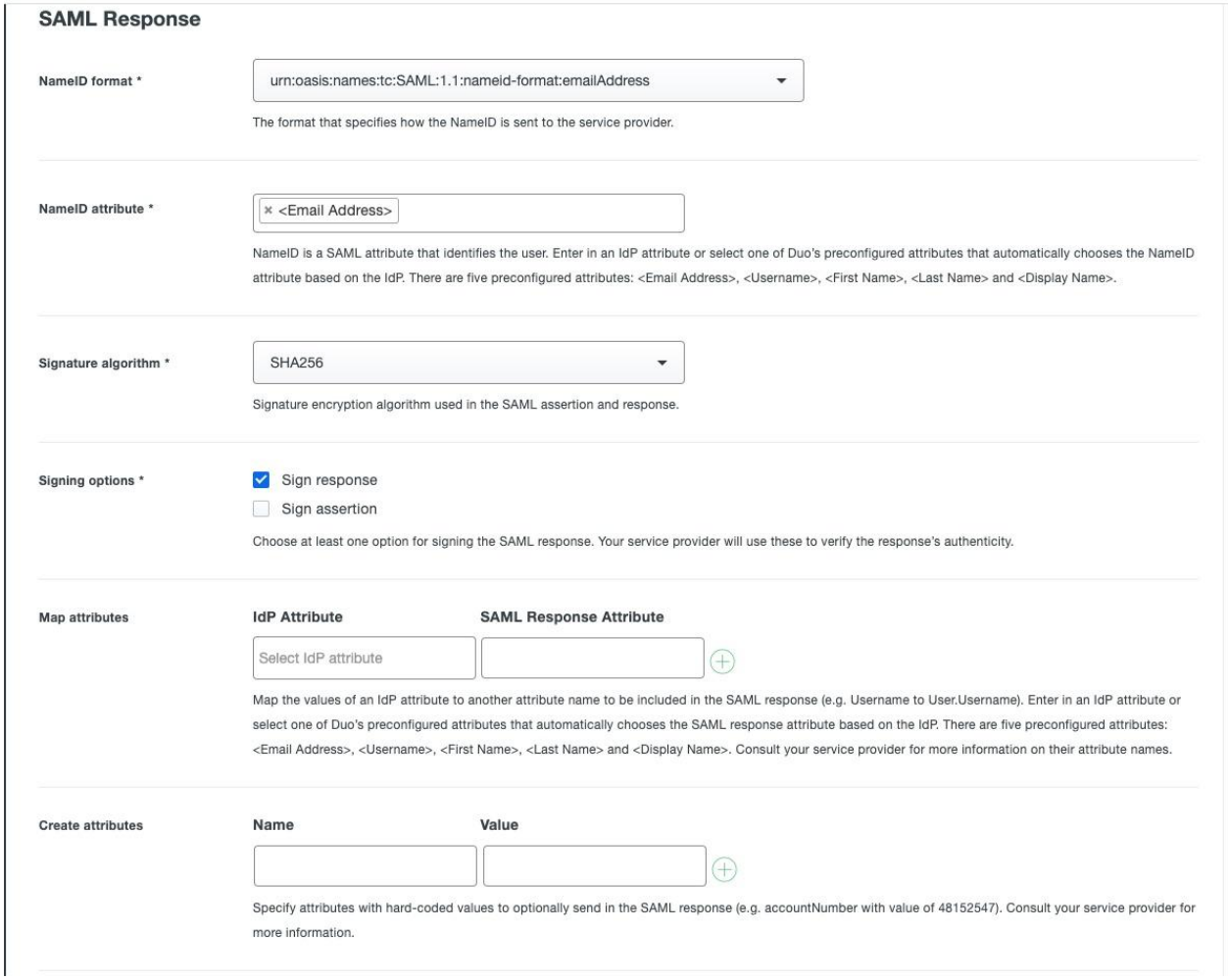
**Assertion Consumer Service (ACS) URL**:
https://enterprise.onna.com/auth/oauth/saml/?acs

**Login URL**: https://enterprise.onna.com/{youraccount}/user/@@login
{youraccount} needs to be replaced by the account name in your Onna URL

**RelayState**:
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)

7) Once the above changes have been saved navigate down to the section SAML Response. The below items will need to be provided:




**NameID format**: "urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress"
**NameID attribute**: email address
**Signing options**: Response

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

**Attributes:**

- **user_id :** email address
- **sn**: last name
- **cn**: first Name
- **email**: email address

8) Finally you will need to ensure the appropriate users or group have been granted access to Onna. Scroll down to the bottom of the page and view the

‘Permitted groups’. Once granted you can click save to apply the above changes.

## 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.