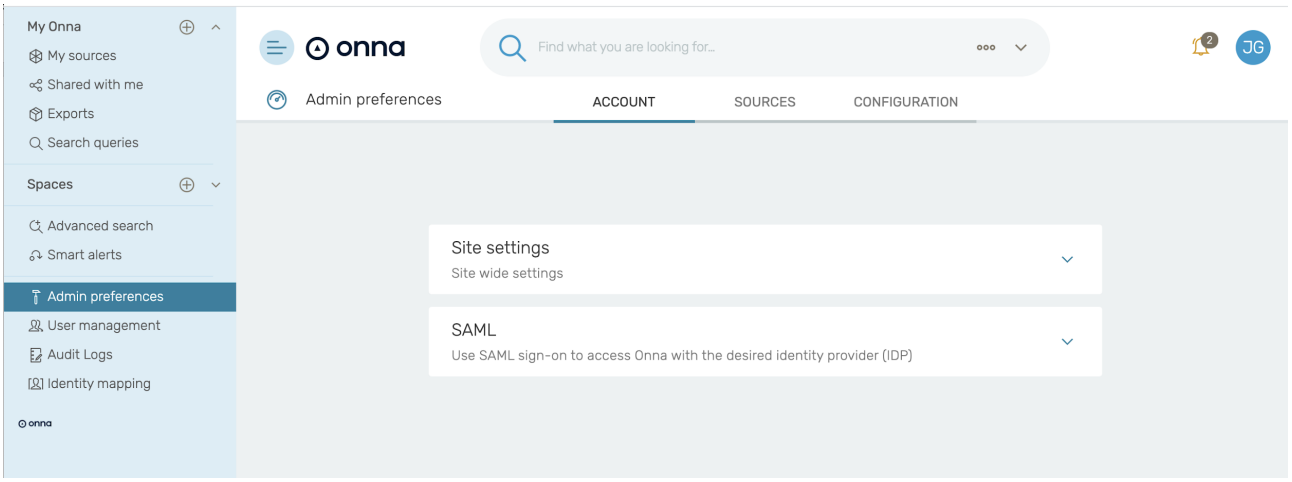
SAML 2.0 Integration

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.

- **Identity provider/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.

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

NOTE: The email address must match the letter 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 the expression as String.toLowerCase(user.email) in **user_id** and **email** attributes to pass lowercase values.

Enabling Sign in through IdP

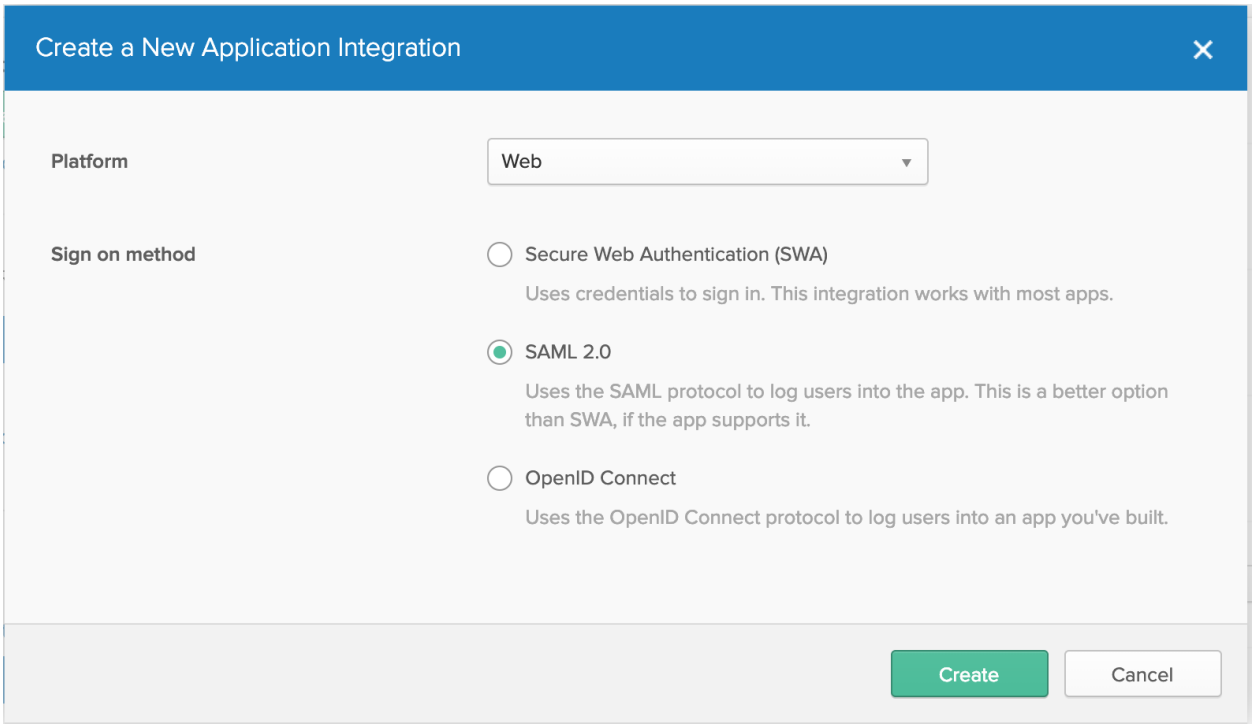
- In order to use an Okta ‘chiclet’ or similar solution, you must provide a value for Default Relay State.

- **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)

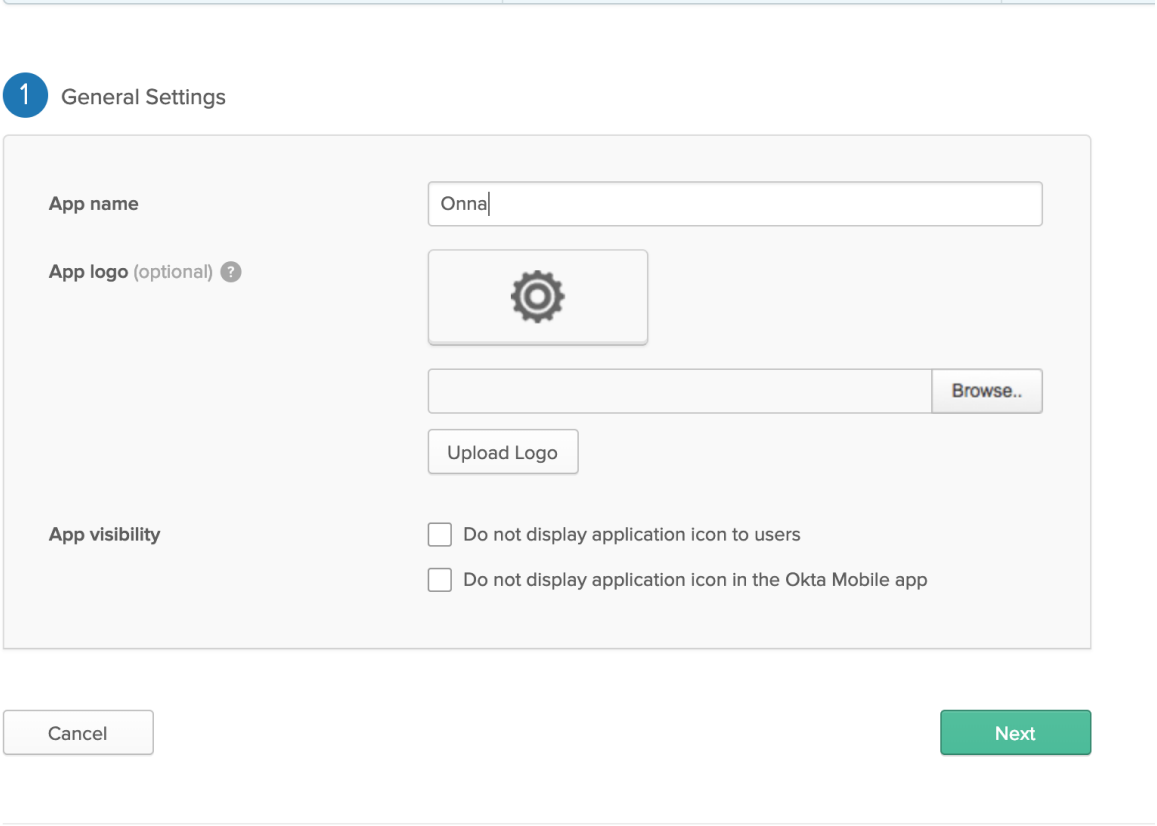
Setting up Okta:

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

1) Create a new SAML 2.0 application in Okta



2) Give your app a name



3) Configure SAML -

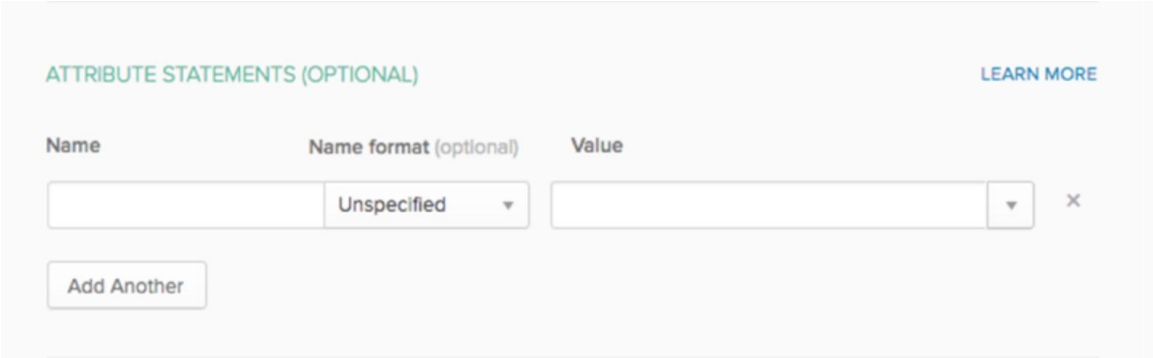
a) There are a few items you need to fill in - please see below.

- **Single Sign-on URL:** https://enterprise.onna.com/auth/oauth/saml/?acs
- **Recipient:** https://enterprise.onna.com/auth/oauth/saml/?acs
- **Destination URL:** https://enterprise.onna.com/auth/oauth/saml/?acs
- **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)
- **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)

4) Only the **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

NOTE: The email address must match the letter 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 the expression as String.toLowerCase(user.email) in **user_id** and **email** attributes to pass lowercase values.



A **SAML Settings**

General

Single sign on URL: https://enterprise.onna.com/auth/oauth/saml/?acs

- [x] Use this for Recipient URL and Destination URL
- [ ] Allow this app to request other SSO URLs

Audience URI (SP Entity ID): https://enterprise.onna.com/auth/oauth/saml/metadata?

Default RelayState: https://enterprise.onna.com/onnapso/signin?idpId=pso-c

If no value is set, a blank RelayState is sent

Name ID format: EmailAddress

Application username: Email

Update application username on: Create and update

Show Advanced Settings

Attribute Statements (optional)

LEARN MORE

Name	Name format (optional)	Value
user_id	Unspecified	user.email
sn	Unspecified	user.lastName
cn	Unspecified	user.firstName
email	Unspecified	user.email

Add Another

SAML Settings

Edit

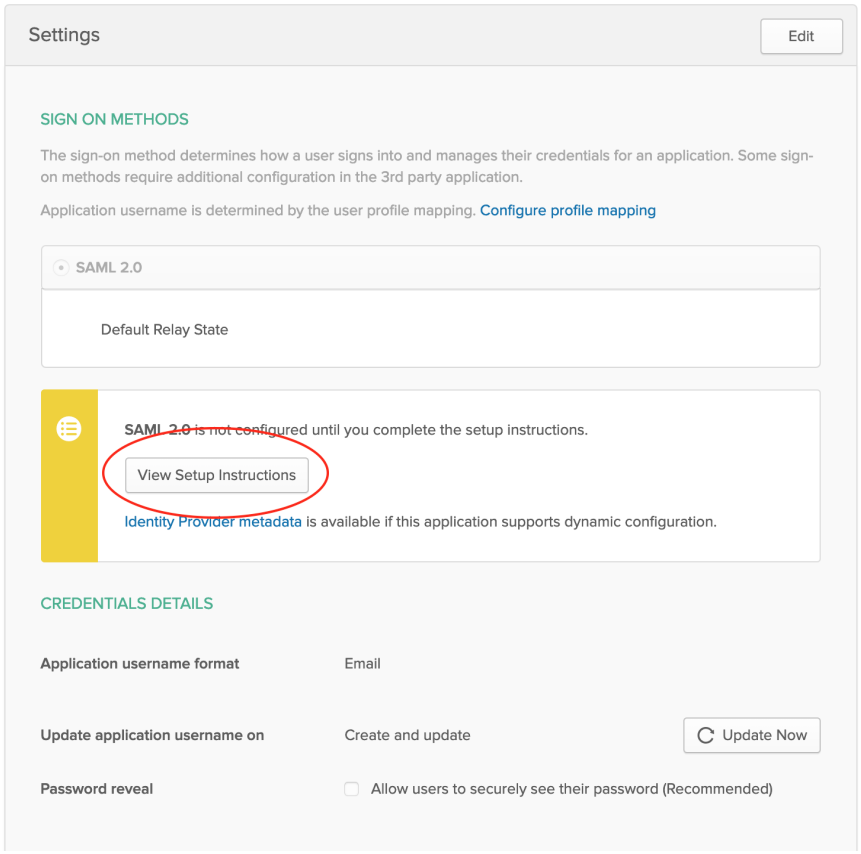
GENERAL

Single Sign On URL	https://enterprise.onna.com/auth/oauth/saml/?acs
Recipient URL	https://enterprise.onna.com/auth/oauth/saml/?acs
Destination URL	https://enterprise.onna.com/auth/oauth/saml/?acs
Audience Restriction	https://enterprise.onna.com/auth/oauth/saml/metadata?idpId=pso-okta
Default Relay State	https://enterprise.onna.com/onnapso/signin?idpId=pso-okta&scopes=onnapso
Name ID Format	EmailAddress
Response	Signed
Assertion Signature	Signed
Signature Algorithm	RSA_SHA256
Digest Algorithm	SHA256
Assertion Encryption	Unencrypted
SAML Single Logout	Disabled
authnContextClassRef	PasswordProtectedTransport
Honor Force Authentication	Yes
Assertion Inline Hook	None (disabled)
SAML Issuer ID	http://www.okta.com/${org.externalKey}

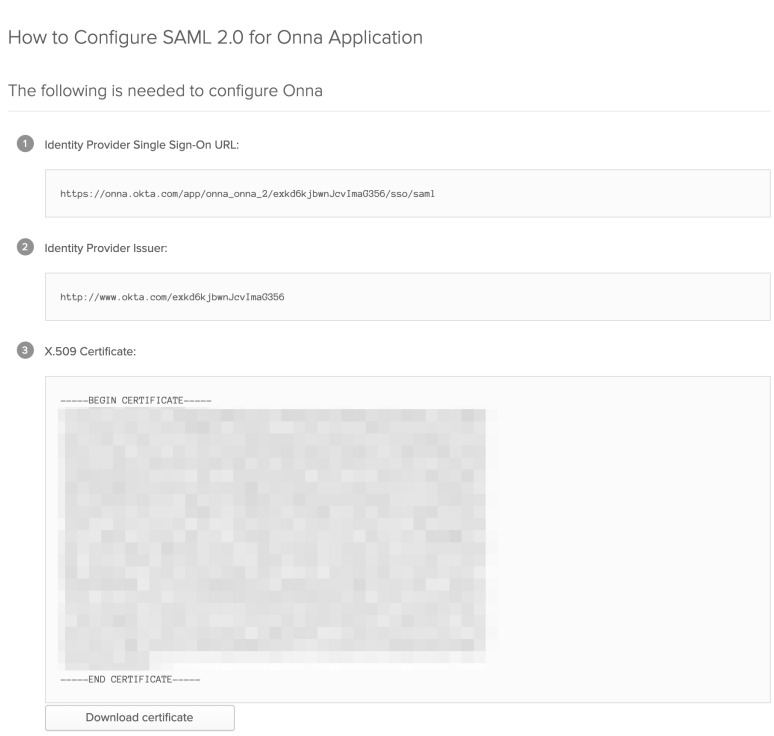
ATTRIBUTE STATEMENTS

Name	Name Format	Value
user_id	Unspecified	user.email
sn	Unspecified	user.lastName
cn	Unspecified	user.firstName
email	Unspecified	user.email

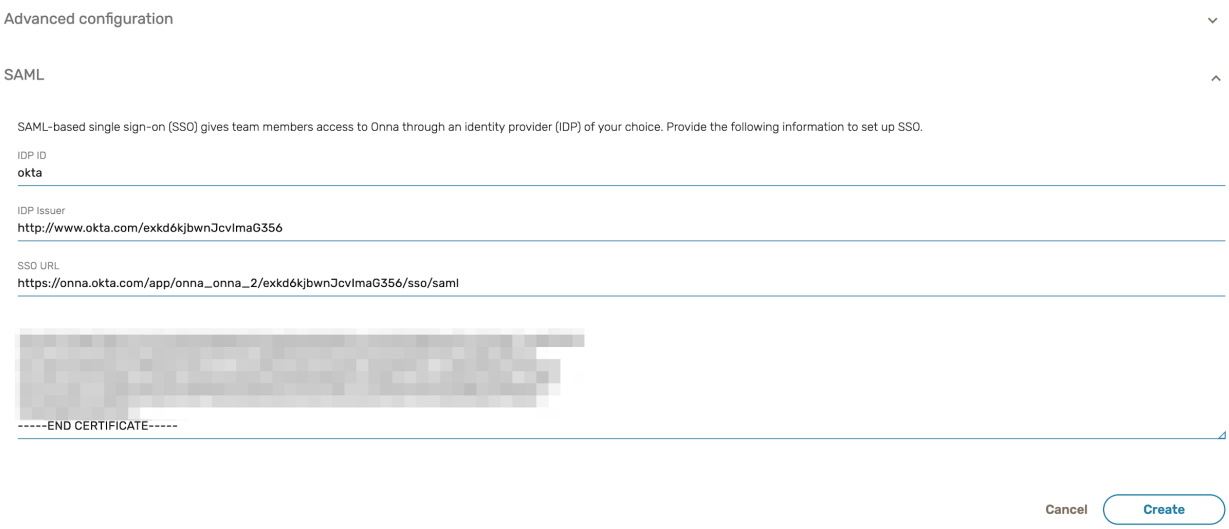
5) The next screen prompts: you are a customer (the rest of the questions are optional)
6) Click the View Setup Instructions button

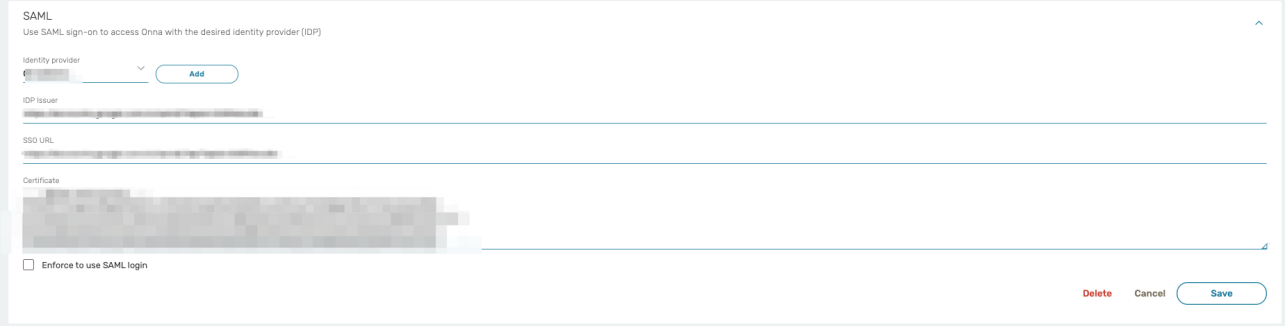


7) Use the values to complete the SSO setup in your Onna configuration



8) In Onna, the completed configuration:





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.