Integrating OnceHub with Okta to allow for SSO

By centralizing authentication with Okta, you ensure that your team can securely access OnceHub using their existing corporate credentials, which enhances security and simplifies the overall login process.

This article guides you through the end-to-end process of creating a SAML 2.0 integration between OnceHub and Okta, from initial app creation to final user assignment and verification.

Step 1: Create a New Application Integration in Okta

In Okta, follow the steps below to create a new SAML application integration:

1. Go to **Applications**.
2. Click **Create New Application**.
3. Select SAML 2.0 as the **Sign on method**.
4. Click **Next**.

Step 2: Configure the General Settings in Okta

In Okta, after successfully creating the SAML 2.0 application, navigate to the **General Settings** tab to configure the primary identification details. Within this section, define an **App name** that clearly identifies the integration within your Okta dashboard (e.g., "OnceHub").

Step 3: Configure the SAML Settings in Okta

To configure the SAML settings within Okta, you will need to enter credentials provided by OnceHub.

Finding the Credentials within OnceHub

In OnceHub, follow these steps to open the SAML Configuration pop-up with the required credentials:

1. Click the Gear icon in the top-right corner.
2. Select **Security (and Compliance)** from the dropdown.
3. Click **Setup** next to **Set up SAML configuration for SSO**.

NOTE: Keep the pop-up open for step 4.

Configuring the SAML Settings within Okta

In Okta, follow the steps below to complete the configuration:

1. Go to the **Configure SAML** tab.
2. Copy over the following details from the OnceHub pop-up:

In Okta	In OnceHub
Audience URI (SP Entity ID)	Identifier URL
Single sign on URL + Select checkbox **Use this for Recipient URL and Destination URL**	ACS URL
[Not required; Okta Refers to ACS URL for this function]	~~Single sign-on URL~~

3. Click **Next**.
4. Click **Finish**.
5. Go to the **Sign On** tab.
6. Scroll to **Attribute statements** box.
7. Expend **Show legacy configuration**.
8. Click **Edit** to the right of **Profile attribute statements** and provide the following details:
   - **Name:** Enter the word email.
   - **Name format:** Select **Unspecified**.
   - **Value:** Select **user.email**.

Step 4: Configure the SAML Settings in OnceHub

After the configuration within Okta is completed, you will now need to enter credentials provided by Okta into your OnceHub account.

Finding the Credentials within Okta

In Okta, follow these steps to access the page containing the necessary credentials:

1. Go to the **Sign On** tab.
2. Select **View Setup Instructions**.

Configuring the SAML Settings within OnceHub

In the SAML Configuration pop-up within OnceHub, follow these steps:

1. Click Continue to go to the Required by OnceHub tab.
2. Copy over the following details from Okta:

In Okta	In OnceHub

Identity Provider Issuer	Entity ID
Identity Provider Single Sign-On URL	IDP single sign-on URL
X.509 Certificate	Public x509 certificate

3. Click **Save & continue**.

!

IMPORTANT: For the Public x509 certificate, include the -----BEGIN CERTIFICATE----- and -----END CERTIFICATE---- - syntax in your selection and paste the entire text into the OnceHub field.

Step 5: Assign the OnceHub SAML 2.0 application to Users in Okta

In Okta, follow the steps below to assign the new OnceHub SAML 2.0 application to the users who will be utilizing SSO to sign into your OnceHub account:

1. Go to the **Assignments** tab.
2. Click **Assign**.
3. Select **Assign to People** from the dropdown.
4. Select the users as required.
5. Click **Done**.

Step 6: Verify the Configuration in OnceHub

In OnceHub, click **Verify** to do the final verification for both OnceHub and Okta. Click **Close** once the verification is successful.

Step 7: Enable SSO for All Users in OnceHub

In OnceHub, once you've verified your SSO configuration, you can toggle on **Enable SSO for all Users**.

!

IMPORTANT: Ensure all OnceHub User profile emails match their Okta profile emails exactly. If they do not match, users will be locked out of their OnceHub profiles. Additionally, OnceHub email addresses cannot be changed once SSO is active.