Integrating OnceHub with OneLogin to allow for SSO

By centralizing authentication with OneLogin, 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 OneLogin, from initial app creation to final user assignment and verification.

Step 1: Create a SAML Custom Connector (Advanced) in OneLogin

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

1. Go to **Administration**.
2. Hover over **Applications** in the top navigation and select **Applications**.
3. Click **Add App** in the top right.
4. Search for and select **SAML Custom Connector (Advanced)**.
5. Provide the **Display Name**.
6. Click **Save** in the top right.

Step 2: Configure the SAML Settings in OneLogin

To configure the SAML settings within OneLogin, 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 during the integration setup.

Configuring the SAML Settings within OneLogin

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

1. Go to the **Configuration** tab of the application you created.
2. Copy over the following details from the OnceHub pop-up:

In OneLogin	In OnceHub
Audience (EntityID)	Identifier URL
ACS (Consumer) URL Validator	ACS URL
ACS (Consumer) URL	ACS URL
[Not Required; OneLogin refers to ACS URL for this function	Single sign-on URL

3. Go to the **Parameters** tab of the application you created.
4. Click **+** on the right side of the screen to create a new Field with the following details:
   - **Name:** email (All lowercase)
   - **Include in SAML assertion:** Enabled
5. Click **Save** in the **New Field** pop-up.
6. Select **Email** in the **Value** dropdown.
7. Click **Save**.
8. Click **Save** in the top-right corner to confirm the configuration.

Step 3: Configure the SAML Settings in OnceHub

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

Finding the Credentials within OneLogin

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

1. Go to the **SSO** tab.

Configuring the SAML Settings within OnceHub

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

1. Clic**k Continue** to go to the **Required by OnceHub** tab.
2. Copy over the following details from OneLogin:

In OneLogin	In OnceHub
Issuer URL	Entity ID
SAML 2.0 Endpoint (HTTP)	IDP single sign-on URL

X.509 Certificate text (Select View Details under X.509 Certificate to view the text)	Public x509 certificate

3. Click **Save & continue**.
4. **Do not** click **Verify**.

!

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 4: Verify the Integration

Before proceeding with the steps below, ensure that your OnceHub and OneLogin accounts use the same email address.

Assigning the Application to Yourself within OneLogin

In OneLogin, you must first follow the steps below to assign the OnceHub application to your user account to verify the integration:

1. Hover over **Users** in the top navigation and select **Users**.
2. Click on your name in the list.
3. Go to the **Applications** tab.
4. Click **+** on the right side of the screen.
5. Select the application you created in the pop-up.
6. Click **Continue**.
7. Click **Save**.

Verifying the Integration within OnceHub

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

Step 5: 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 OneLogin 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.

Step 6: Assign the OnceHub SAML 2.0 application to Users in OneLogin

In OneLogin, 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. Hover over **Users** in the top navigation and select **Users**.
2. Click on a user that will use SSO.
3. Go to the **Applications** tab.
4. Click **+** on the right side of the screen.
5. Select the application you created in the pop-up.
6. Click **Continue**.
7. Click **Save**.