Integrating OnceHub with Microsoft Entra ID to allow for SSO

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

Step 1: Create a New Application Integration in Entra ID

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

1. Select **Enterprise apps** from the left navigation menu.
2. Click **New application** in the top left of the screen.
3. Click **Create your own application** in the top left of the screen.
4. Provide a name for the app.
5. Select **Integrate any other application you don't find in the gallery (Non-gallery)**.
6. Click **Create**.

Step 2: Set Up the SAML Configuration in Entra ID

To configure the SAML settings within Entra ID, 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**.

Setting Up the Basic SAML Configuration within Entra ID

In Entra ID, follow the steps below to complete the configuration:

1. Click **Single sign-on** from the left navigation menu of the created app.
2. Select **SAML** as the sign-on method.
3. Click **Next**.
4. Click **Edit** in the **Basic SAML Configuration** tile.
5. Copy over the following details from the OnceHub pop-up:

In Entra ID	In OnceHub
Microsoft Entra Identifier	Identifier URL
Reply URL	ACS URL
Sign on URL	Single sign-on URL

6. Click **Save**.

Setting Up the User Attributes & Claims within Entra ID

In Entra ID, follow the steps below to complete the configuration:

1. Go to the previous page in your browser (The **Single sign-on** page).
2. Click **Edit** in the **User Attributes & Claims** tile.
3. Click **Add new claim** in the top left of the screen.
4. Enter the word **email** as the name.
5. Expand Claim conditions and add the following 2 conditions:

User type	Scoped Groups	Source	Value
Members	Leave as is.	Attribute	user.userprincipalname
All guests	Leave as is.	Attribute	user.mail

6. Click **Save**.

Step 3: Configure the SAML Settings in OnceHub

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

Finding the Credentials within Entra ID

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

1. Go to the previous page in your browser (The **Single sign-on** page).
2. Download the **Certificate (Base64)** in the **SAML Signing Certificate** tile.
3. Scroll down to the **Set up {Your App Name}** tile to use in the steps below.

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 Entra ID:

In Entra ID	In OnceHub
Microsoft Entra Identifier	Entity ID
Login URL	IDP single sign-on URL
Certificate (Base64) text	Public x509 certificate

3. Click **Save & continue**.

!

IMPORTANT: You can use a text editor such as Notepad to open the Certificate (Base64) and copy over the text. It must include the -----BEGIN CERTIFICATE----- and -----END CERTIFICATE----- syntax in your selection.

Step 4: Assign the OnceHub SAML 2.0 application to Users in Entra ID

In Entra ID, 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. Select **Enterprise apps** from the left navigation menu.
2. Open the application you created for OnceHub.
3. Click **Users and groups** from the left navigation menu of the created app.
4. Click **Add user/group** in the top left of the screen.
5. Under **Users**, click **None Selected**.
6. Select the user.
7. Click **Select**.
8. Click **Assign**.

Step 5: Verify the Configuration in OnceHub

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

Step 6: 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 Entra ID 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.