Configuring single sign-on (SSO) for your account

Signing in with single sign-on (SSO) is a feature designed specifically for organizations using an identity provider across their organization to regulate signing into all their third-party apps through SSO.

Requirements

To configure SSO in your account, you must be a OnceHub Administrator. However, you do not need a product license. Learn more

You must already have an account through an identity provider (IDP) such as Okta, OneLogin, Azure, or G Suite. You can also configure SSO if you have G Suite, without installing through the G Suite Marketplace.

> **Note:**
>
> If you set up SSO for your OnceHub account, you cannot set session policies or lockout policies. Users also cannot set up 2-factor authentication in OnceHub.

Fields mapped

This article includes guidelines on configuring SSO in OnceHub and your IDP.

Some are grabbed in OnceHub and entered in your IDP's admin area. Others are grabbed from your IDP and added to OnceHub.

From OnceHub to your IDP

Identifier URL

A unique string identifying the provider issuing a SAML request. This is usually in URL format. It is not always required by providers.

Sometimes called the **Entity ID** in various IDPs.

ACS URL

An Assertion Consumer Service (ACS) that provides the location where OnceHub accepts the SAML response, for the purpose of establishing a session based on an assertion.

With some IDPs, such as Okta, you will use the OnceHub **ACS (Assertion Consumer Service) URL** as the value for the **Single sign-on URL** field in your IDP. This could also be called the **Reply URL**.

This same value can also be used for the **Recipient URL** and **Destination URL** in your IDP.

Single sign-on URL

The URL for signing into your OnceHub account.

Sometimes this is called the **Login URL** (Azure)**, Login redirect URL** (Okta), or something similar.

Unique ID

A unique identifier attribute in your IDP.

You will be mapping the attribute **email** (letters all in lower-case) to your employee/user email field.

From your IDP to OnceHub

Entity ID

A unique string identifying the provider issuing a SAML request. This is usually in URL format. It is not always required by providers.

Sometimes called the **Identifier** or **Identifier URL** in your IDP.

IDP single sign-on URL

© Copyright OnceHub 2025. All rights reserved.

The URL for signing into your IDP.

Sometimes this is called the **Login URL** (Azure)**, Login redirect URL** (Okta), or something similar.

Public x509 certificate

A digital certificate in the x509 PKI standard, used to sign SAML requests, responses, and assertions between OnceHub and your IDP.

You will copy and paste the certificate in full within OnceHub, including the text for **-----BEGIN CERTIFICATE-----** and **-----END CERTIFICATE-----** .

1. Request access

SSO is intended for accounts with multiple users who take the extra security measure of signing into third-party applications using an identity provider. Please contact us to learn more. OnceHub can enable the SSO functionality in your account manually.

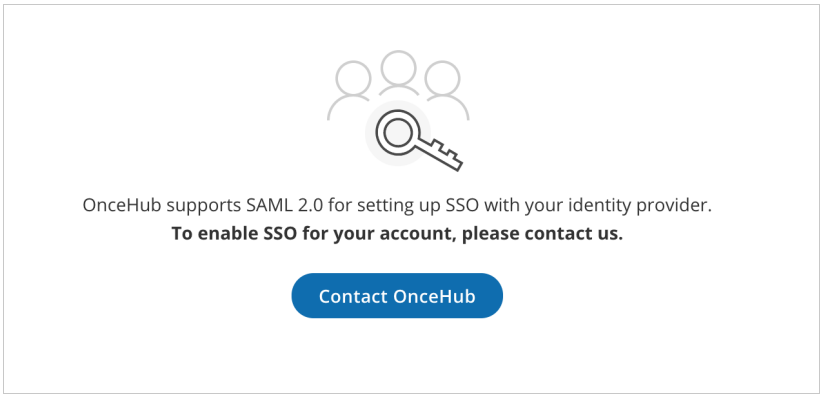

Figure 1: Contact us to enable SSO for your account

2. SAML configuration

You can access SAML configuration at OnceHub **Account settings** -> In the lefthand sidebar, select **Security** -> **SSO**.

OnceHub provides specific field values you can copy and configure within your identity provider.

This includes an **Identifier URL**, **ACS URL**, **Single sign-on URL**, and **Unique ID**.

Next, you will need to map unique ID attributes. The attribute **email** with all lower-case letters should be mapped to your employee/user email field.

3. Required by OnceHub

You will need specific field values from your identity provider you can copy and configure within OnceHub.

This includes an **Entity ID**, **IDP single sign-on URL**, and **Public x509 certificate**.

© Copyright OnceHub 2025. All rights reserved.

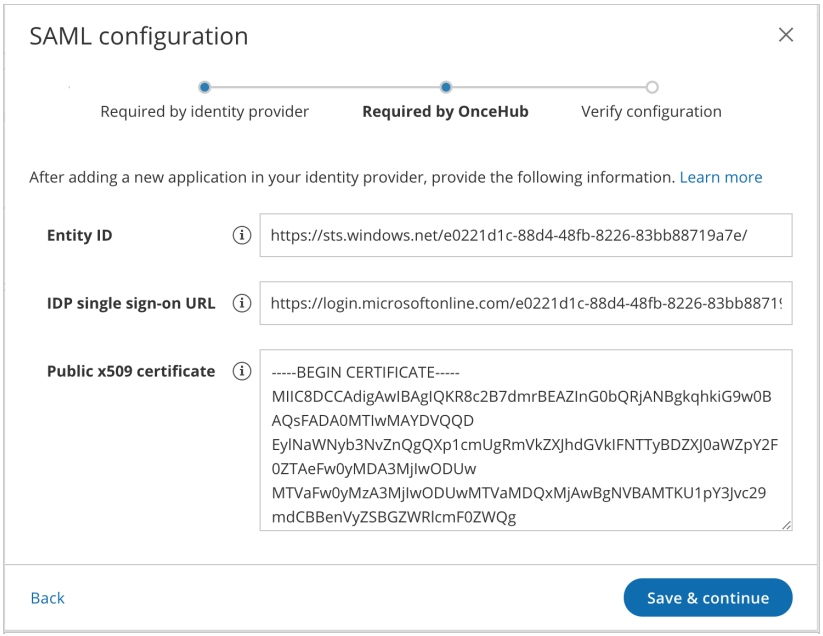

Figure 2: Required by OnceHub - Example uses Azure Active Directory credentials.

4. Verify configuration

OnceHub will speak to your identity provider and verify that the configuration has the correct values on both sides to proceed.

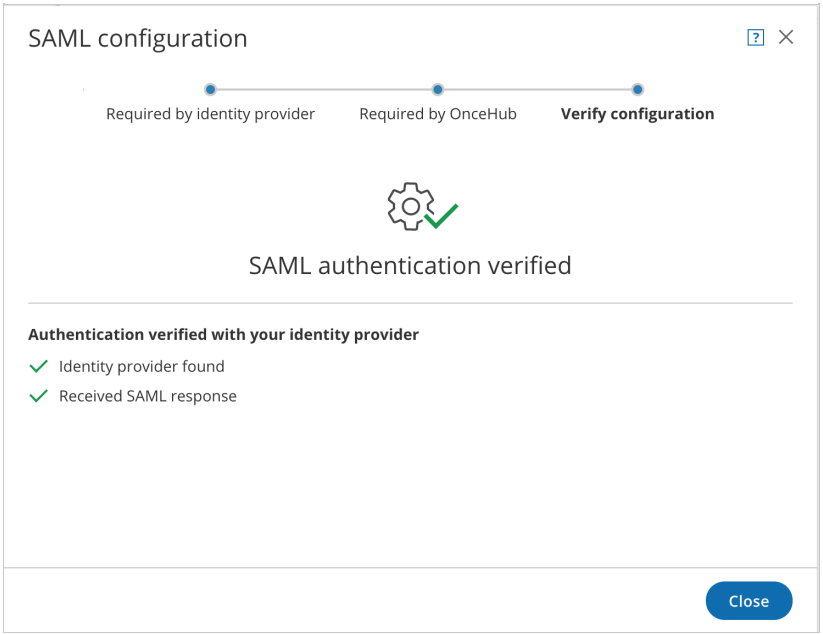

Figure 3: Verify configuration

5. Enable SSO for all users

Once you've verified your SSO configuration, you can select the **Enable SSO for all users** toggle. All Users in your OnceHub account can now access their account using SSO.

Important:

Before you enable the account, make sure all your Users have matching email addresses for their OnceHub User profile and their IDP profile.

© Copyright OnceHub 2025. All rights reserved.

Once SSO is enabled, they **will not** be able to change their OnceHub email.

If their OnceHub email does not match the email in their IDP profile, they **will not** be able to log in.

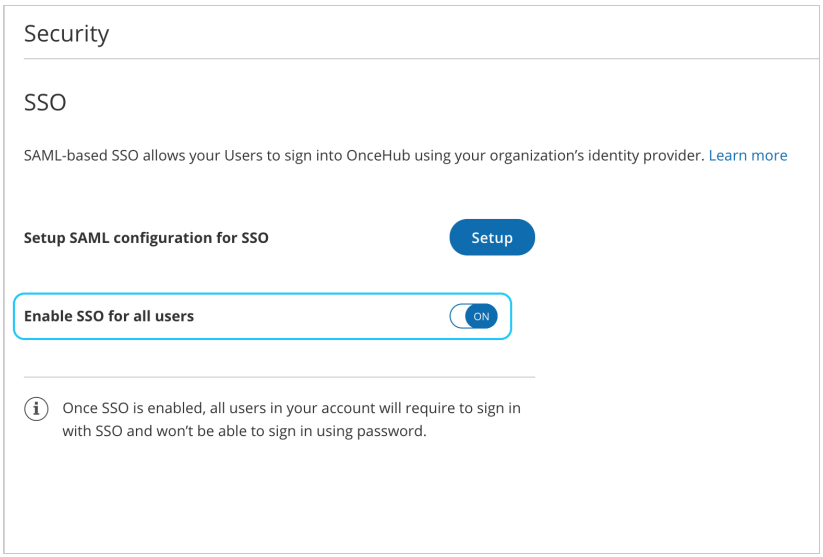

Figure 4: Enable SSO for all users

Note:

If existing Users were already signing into OnceHub using an email and password, they will no longer be able to do so. They will only be able to sign in using SSO.

© Copyright OnceHub 2025. All rights reserved.