Configuring single sign-on (SSO) for your account

Single Sign-On (SSO) allows your users to securely access OnceHub using their existing identity provider (IDP) credentials, simplifying login and enhancing security. This guide outlines the steps to configure SSO (specific instructions for IDPs, like OneLogin, Azure, Okta, and G Suite) and how to manage and utilize SSO effectively.

What is SSO and Why Use It?

Single Sign-On (SSO) enables users to log in to OnceHub without creating a new password. Instead, authentication is handled by your identity provider (IDP), such as OneLogin, Azure AD, G Suite, or Okta.

Benefits of Using SSO:

- **Simplified User Experience:** Users can access OnceHub using their IDP credentials without needing separate login details.
- **Enhanced Security:** Centralized authentication reduces the likelihood of password-related vulnerabilities.
- **Streamlined User Management:** Administrators control access and permissions through the IDP.

Prerequisites for SSO Configuration

Before configuring SSO, ensure you meet the following requirements:

- **OnceHub Account:** You must be an administrator in your OnceHub account.
- **Security and Compliance Add-On:** Your account must have the **Security and Compliance Add-On** activated.
- **Identity Provider (IDP):** Have an active account with an IDP (e.g., OneLogin, Azure AD, Okta, or G Suite).
- **Matching Email Addresses:** User email addresses in your IDP must match their OnceHub user profiles. If they don’t match, users will be unable to log in.

General SSO Setup Process

Regardless of the identity provider, the general SSO configuration process in OnceHub involves these steps:

1. **Request Access to SSO:**
    - SSO is available for organizations with the Security and Compliance Add-On. Contact OnceHub support to enable SSO for your account.
2. **Navigate to SAML Configuration:**
    - Click on the gear icon in the top-right, then Security and Compliance.
3. **Obtain Required Fields from Your IDP:**
    - You will need the following from your IDP:

    - Entity ID (or Identifier)
    - Single Sign-On URL (Login URL)
    - Public x509 Certificate
  - These fields may have different names depending on your IDP.

4. **Enter IDP Details in OnceHub:**
    - Copy the required fields from your IDP and paste them into OnceHub's SAML configuration fields.

5. **Verify and Test Connection:**
    - Click Verify in OnceHub to confirm the SAML configuration works correctly.
    - Ensure that the test user can log in successfully using SSO.

6. **Enable SSO for All Users:**
    - Once the configuration is verified, toggle the Enable SSO for All Users option. This requires all users to log in using SSO.

Provider-Specific Configuration Steps

Configuring SSO with OneLogin

1. In OneLogin:
    - Go to Administration → Applications .
    - Search for SAML Test Connector (Advanced) and start setup.
    - Configure key fields:
        - Entity ID : Add the OnceHub-provided Entity ID.
        - SAML SSO URL : Copy OnceHub's login URL into the connector.

2. Generate x509 Certificate:
    - Click Certificate Settings in OneLogin and download the x509 certificate.

3. In OnceHub:
    - Enter the Entity ID, SSO URL, and public x509 certificate in Account Settings → Security → SSO .

4. Verify and enable the integration as described above.

Configuring SSO with G Suite

- In G Suite Admin Console:
    - Go to Apps → SAML Apps → Add App .

    - Add custom app settings:
        - SSO URL : Copy OnceHub's SAML login URL.
        - Entity ID : Input the unique OnceHub identifier.
    - Download the x509 certificate provided by G Suite.
- In OnceHub:
    - Paste the SSO URL, Entity ID, and x509 certificate into the SAML configuration settings.
    - Test the connection and verify functionality.

Configuring SSO with Okta

- In Okta:
    - Go to Applications → Add Application .
    - Search for SAML-based Application and select it.
    - Add app details, including:
        - Entity ID and Login Redirect URL (provided by OnceHub).
    - Ensure attributes such as email are mapped correctly.
- Download Certificate:
    - Generate and download the x509 certificate from Okta.
- In OnceHub:
    - Input the required fields (x509 certificate, Entity ID, SSO URL).
    - Test and enable the integration.

Configuring SSO with Azure AD

- In Azure Portal:
    - Go to Enterprise Applications and create a new application for OnceHub.
    - Add SAML configuration:
        - Identifier (Entity ID) : Use OnceHub's Entity ID.
        - Reply URL : Add the OnceHub Login Redirect URL.
- Download Certificate:
    - Download the x509 certificate and ensure claims are set to include email.
- In OnceHub:

- Enter the details for Entity ID, SSO URL, and x509 certificate.
- Test the integration before enabling SSO for all users.

Using SSO in Your Organization

Once SSO is configured, users in your organization can log in securely using the following steps:

1. Go to the OnceHub login page.
2. Click Sign in with SSO.

Common SSO Management Tasks

Reset or Modify SSO Configuration

If your IDP changes settings like the Entity ID or SSO URL, you must update the modified fields and verify settings in OnceHub to ensure SSO continues to function.

Removing a User or Role in the IDP

- If a user no longer requires OnceHub access, remove them from your IDP or disable their role.
- The changes will reflect in OnceHub, blocking access for the user.

Troubleshooting SSO Login Issues

Common issues include:

- **Email Mismatches:** Ensure the user’s email in the IDP matches their email in OnceHub.
- **SSO Certificate Expiry:** Renew the x509 certificate in your IDP and update it in OnceHub.
- **Incorrect Mapping:** Recheck attribute mappings (e.g., email) to ensure they are set correctly.

Frequently Asked Questions (FAQs)

Can I enable SSO for some users and not others?

No. Once SSO is enabled, it becomes the sole login method for all users in your account.

What happens if a user cannot log in via SSO?

- Ensure their OnceHub email matches their email address in the IDP.
- Check if their role in the IDP allows access to the OnceHub application.

How do I disable SSO?

Toggle off the **Enable SSO for all users** option. This allows users to log in using their OnceHub credentials again.