Security settings

Understand all the security settings you can customize for your account.

SSO

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. This may include identity providers such as:

- Okta
- OneLogin
- Azure
- G Suite

To use SSO to sign into OnceHub, your OnceHub Administrator must have already configured SSO for your account.

To access your OnceHub account, click the **Sign in with SSO** link at the bottom of the OnceHub sign-in page.
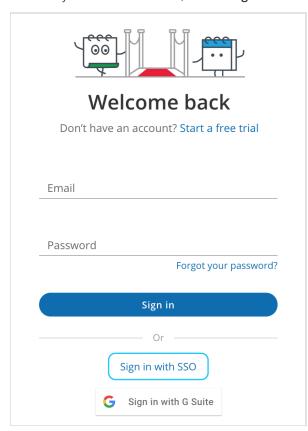

Figure 1: Sign in with SSO

You will provide your email and be redirected to your identity provider. Once authenticated, you'll be returned to your signed-in OnceHub account.

If you're having difficulty signing in, please don't hesitate to contact us for more help.

Password policies

Help Article

Using a strong password is an important safety measure that protects your account. Setting a password policy can ensure that Users in your account follow password best practices and organizational guidelines.

You must be a OnceHub Administrator to make changes to password policies. However, you do not need an assigned product license. Learn more

Password policy changes are enforced when the User creates or changes their password. To ensure that new password policies are quickly propagated throughout the account, you should set a seven day expiration time frame. This will force users to comply with your password policy within a week. Then, you can extend the expiration time frame to expire after 6 to 12 months.

> ⓘ **Note:**
>
> Password policies apply to Users in your OnceHub account that use an email and password combination to login. Passwords for Users with a G Suite login are managed by Google. Learn more about Google password policies

Customizing Password policies

1. In the top navigation menu, click the gear icon → **Security** → **Password policies**.
2. By default, all passwords in OnceHub must be at least six characters long and include both lower case letters and numbers. Adjust your policy to accommodate for stricter requirements and click **Save**.

There are four parameters available to an admin:

Password length

This defines the minimum character length for the password. Passwords must contain at least the number of characters defined by the password length. The longer a password, the more secure it is. Enforcing a long password is recommended.

Password complexity

This defines which groups of characters must be used to construct a password. To meet the requirement, a password must contain at least one letter from each of the enabled groups. The special characters group follows best practices and contains the characters recommended by OWASP.

Password expiration

Periodically changing your password is a recommended practice. By default, passwords do not expire in OnceHub. However, enabling password expiration forces Users to change passwords. If a password age is older than the expiration timeframe, your Users will be prompted to select a new password on their next login.

Password history

This section determines whether Users can reuse previous passwords when they change their passwords. Many Users want to reuse the same password for their account over a long period of time, but the longer a password is in use, the less it is secure. If Users are required to change their password, but they can reuse an old password, the effectiveness of a good password policy is greatly reduced.

> ⓘ **Note :**
>
> Users can only edit their own passwords. Administrators cannot edit other passwords of other Users.

Account lockout policies

Account lockout protects against brute force login attempts and automatically suspends account access when multiple

failed login attempts have been identified.

Locked accounts prevent access to the User application. A locked account is able to accept bookings from Customers and Booking pages function as normal. If a User is locked out of their account, all Administrators receive an email notification advising about the security event.

Requirements

You must be a OnceHub Administrator to make changes to password policies. However, you do not need an assigned product license. Learn more

> ⓘ **Note :**
>
> Account lockout applies to all Users on your OnceHub account that use an email and password combination to login. This means if a User signs in through SSO or G Suite, the OnceHub Administrator cannot set account lockout policies for that account.
>
> Account activity for Users with a G Suite login is monitored by Google. Learn more about G Suite activity alerts

Customizing Account lockout policies

1. In the top navigation menu, click the gear icon → **Security → Account lockout policies**.
2. By default, account lockout is disabled. Enable the account lockout and define the lockout criteria. Enabling Account lockout is a good security practice. We recommend setting the lockout criteria to five attempts within 30 minutes.

   - **Login attempts allowed** - The number of unsuccessful login attempts required to lock an account.
   - **Lockout timeframe** – The timeframe for counting unsuccessful login attempts.
     The lockout criteria determines the threshold that triggers lockout. Suppose your Account lockout policy is set to allow no more than three attempts in 60 minutes. Three failed login attempts at 09:00 am, 09:30 am and 09:59 am will lockout your account (since all three attempts happened within the lockout timeframe). Three failed login attempts at 09:00 am, 09:30 am and 10:01 am will not lockout the User account (since only two attempts were in the lockout timeframe).

3. Click **Save**.

> ⓘ **Note:**
>
> When an account is locked, Administrators can unlock all User accounts apart from their own. To unlock a User account, click on your profile image or initials in the top right corner and select **Users**. Select **Unlock account** from the action menu of a specific User. If you are the only Administrator and your account has been locked, please contact us.

Session policies

OnceHub recommends the implementation of short sessions, a security feature that protect your account from unauthorized access by triggering an automatic timeout after a period of inactivity.

By default, OnceHub can automatically keep accounts signed in for up to 14 days. This is a convenience mechanism for Users who typically access their account from home and do not share their devices with other individuals.

Requirements

You must be a OnceHub Administrator to make changes to password policies. However, you do not need an assigned product license. Learn more

> ⓘ **Note:**
>
> Session policies are not available for Users signed in via G Suite or SSO.

Customizing Session policies

1. In the top navigation menu, click the gear icon → **Security → Session policies**.

2. By default, session timeout is disabled. If a short session duration is part of your organizations information security policy, you can use Short session settings to enforce this for all Users across the account

3. Adjust your policy and click **Save**.

CAPTCHA

In this section, you can enable CAPTCHA for your account's booking actions. This confirms your page is being booked by a human rather than a bot.

Enabling CAPTCHA adds a strictly necessary cookie named **cf_chl_prog**. This cookie is created and used by Cloudflare to execute Javascript or CAPTCHA challenges, identifying trusted web traffic for your pages. It does not identify the person receiving the cookie on the web application, track them, or store their personal identification details in any way. It is never used beyond the scope of the CAPTCHA challenge.

Learn more: What is a strictly necessary cookie?