OnceHub Support

Session policies

Last Modified on Nov 7, 2024

OnceHub recommends the implementation of Short sessions. Short sessions are a security feature that protect your OnceHub account from unauthorized access. With Short sessions enabled, an automatic timeout is triggered 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.

If you share your device, or you access your account from a public location, automatic sign-in is not recommended. For example, if you work in an office with heavy footfall and your account remains logged in at an unattended desk, there is a risk that an unauthorized individual could gain access to your computer.

To prevent automatic sign-in, you should enable Short sessions. With Short sessions enabled, your account will automatically timeout after a period of inactivity. We recommend setting the maximum idle session duration to 30 minutes. In this case, any action performed after 30 minutes of inactivity will automatically redirect you to the login page and prompt you for your login details.

In this article, you will learn about customizing the Session policies page for your OnceHub account.

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**.