OnceHub Support

Account lockout policies

Last Modified on Oct 13, 2022

Account lockout provides an additional layer of security for your OnceHub account. It 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.

In this article, you will learn how to customize the Account lockout policies 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 :

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.