OnceHub Support

Password policies

Last Modified on Oct 13, 2022

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.

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

Skip ahead to:

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 the OnceHub Administrator in the Password policies section:

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. Here you can determine whether Users can reuse previous passwords, and if so, how many times they must change their password before reusing one.

Note :

Users can only edit their own passwords. Administrators cannot edit other passwords of other Users. Learn more about changing your password