Set up two-factor authentication

Last Modified on Aug 13, 2020

Enabling two-factor authentication adds an extra layer of security to your account. You can set up two-factor authentication for yourself in the **Authentication** section of your User profile.

When two-factor authentication is enabled, you'll sign in to your account in two steps using your OnceHub account password and a unique verification code sent to your mobile phone.

In this article, you'll learn about enabling two-factor authentication, the sign in process when two-factor authentication is enabled for your profile, and the two-factor authentication lockout policy.

> **Note:**
>
> Two-factor authentication is not available for Users signed in via G Suite or SSO.

Who can set up two-factor authentication?

Any User can enable two-factor authentication for their own profile.

OnceHub Administrators cannot enable two-factor authentication for another User. However, they can disable two-factor authentication for any User. To disable two-factor authentication for another User, the Administrator will be required to provide their OnceHub password.

Setting up two-step authentication

1. Sign in to your OnceHub Account.
2. Open the left navigation bar and go to **Profile -> Authentication** (Figure 1).

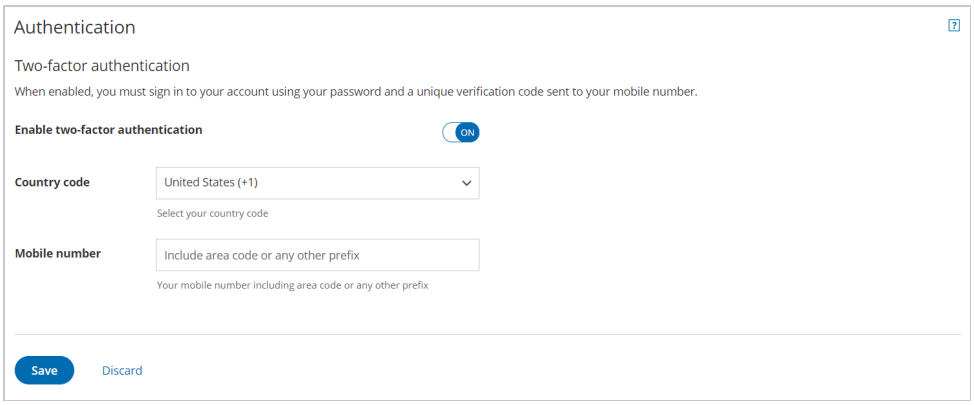

Figure 1: Authentication section

3. Toggle the **Enable two-factor authentication** field **ON**. The **Password required** pop-up appears.

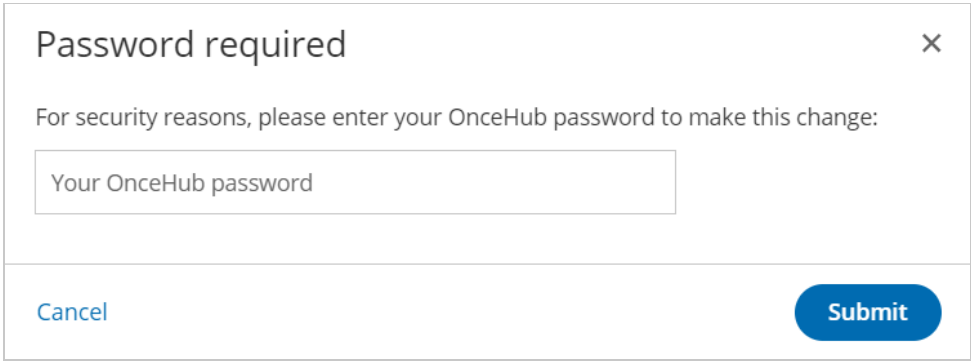

Figure 2: Enter your password

4. Enter your OnceHub password to confirm that you want to enable two-factor authentication.
5. Click **Submit**.
6. Next, select your **Country code** from the drop-down. By default, the country code is selected based on your profile's time zone settings.
7. Enter your **Mobile number.**
8. Click **Save.** A unique 6-digit verification code is sent via SMS to the mobile number you provided. This is done to verify that the mobile number is correct, and that you can receive the SMS. If you do not receive a code, click **Resend**.
9. Enter the verification code you just receive in the **Verify your mobile number** pop-up that appears (Figure 3).

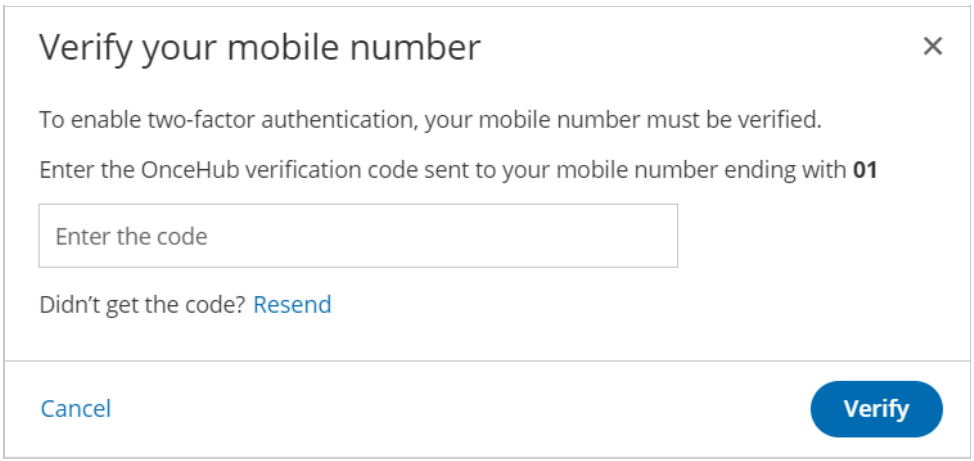

Figure 3: Verify your mobile number

10. Click **Verify**. If your mobile number is successfully verified, two-factor authentication will be enabled for your profile.

You will now sign in to your account in two steps. Learn about signing in with two-factor authentication.

Note:

Two-factor authentication has a built-in lockout policy to detect irregular activity. If any irregular sign-in activity is detected, your account will be locked. If your account is locked, contact your account Administrator to unlock it.