# How does Two-Factor Authentication (2FA) work in DrChrono?

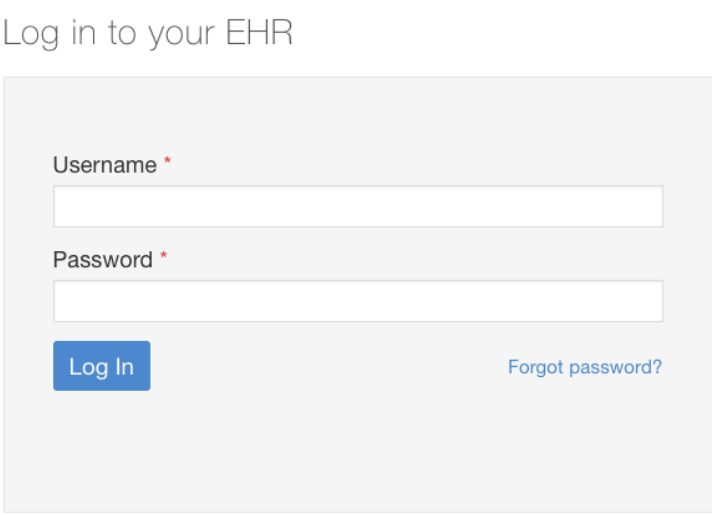
Last modified on 07/21/2025 12:29 pm EDT

Two-factor authentication (2FA) helps secure your account by linking a mobile device to your login credentials. Your mobile device is then used to generate an authentication token that a user must enter while logging in. This adds an extra layer of security so that someone cannot simply obtain your username and password to log into your account and access your data.

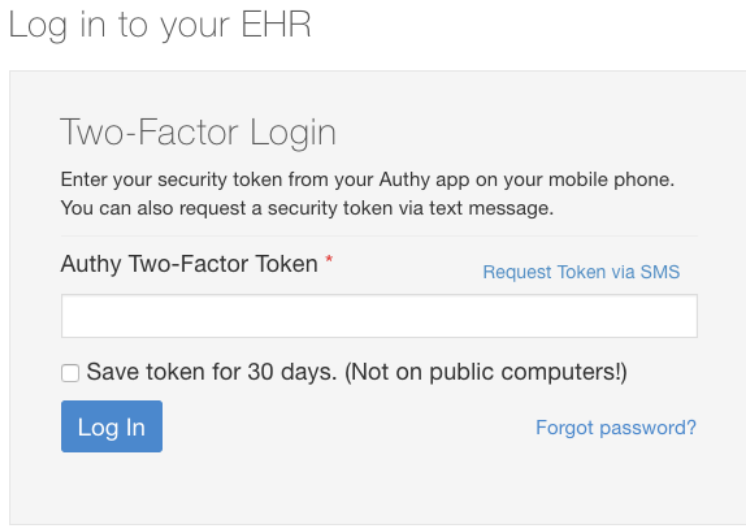
To use 2FA, you will need to complete the setup process illustrated in this guide.

## Logging in with 2-Factor Authentication

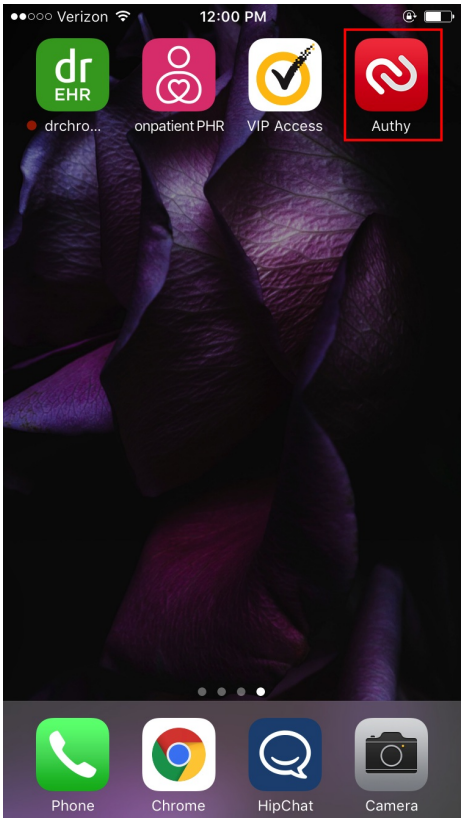
1. Visit the DrChrono log in page. Enter your credentials and select the **Log In** button.




2. After entering your credentials, a page will appear asking for a two-factor authentication token. For this step, you will need your mobile phone. You will need either the Authy app installed or select the **Request Token via SMS** button to continue.

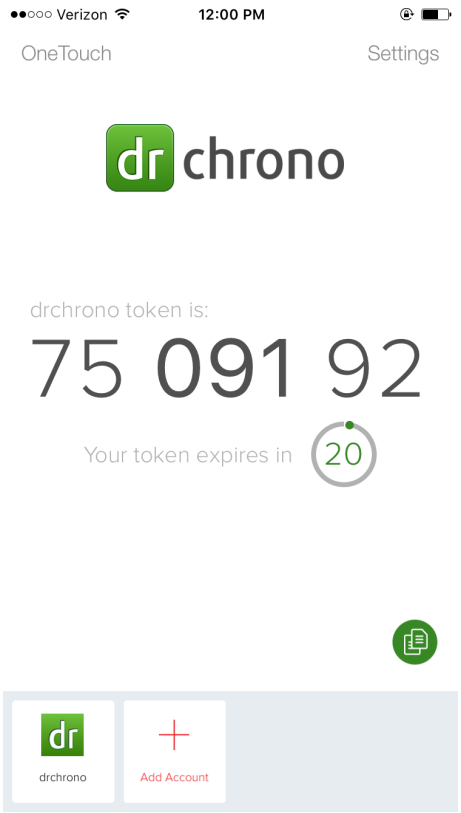



3. On your mobile device, open the Authy app or check your text messages for an authorization code.




4. If you are using Authy, enter the seven-digit code displayed on the screen. If your Authy app does not look like this page, make sure that you have linked your DrChrono account to Authy and that DrChrono is selected as the account at the bottom of the page.

**Note:** Only the mobile version of the Authy app is authorized for use with DrChrono 2FA. The desktop app is no longer supported.



5. Mobile logins only. If you log into DrChrono on a mobile device, you may select the**Copy** button to copy this code to the clipboard. This allows you to quickly paste your code into the 2-factor authentication page.



6. Type or paste your authorization code into the **Authy Two-Factor Token** box. Select **Log In** to log in to DrChrono.

