How do I set up Two-Factor Authentication (2FA) in my account?

07/08/2024 7:59 pm EDT

What is Two-Factor Authentication (2FA)?

Two-Factor Authentication (2FA) is a security measure that safeguards your account in the event your login credentials become compromised. With 2FA, **your mobile device becomes linked to your login credentials and is used to generate or receive an authentication token** that a user must enter while logging in.

This adds an extra layer of security so that a malicious user must obtain both your login credentials and access to your mobile device to access your account.

Two-Factor Authentication (2FA) is available on all plan types for provider and staff accounts in DrChrono. For information on requiring 2-factor authentication for your staff members, see our article How do I set up Two-Factor Authentication (2FA) for a staff member?

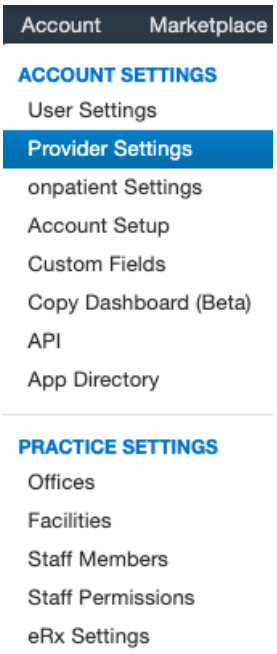
Note: Only the mobile version of the Authy app is authorized for use with DrChrono 2FA. The desktop app is no longer supported.

Setting Up Two-Factor Authentication (2FA) in DrChrono

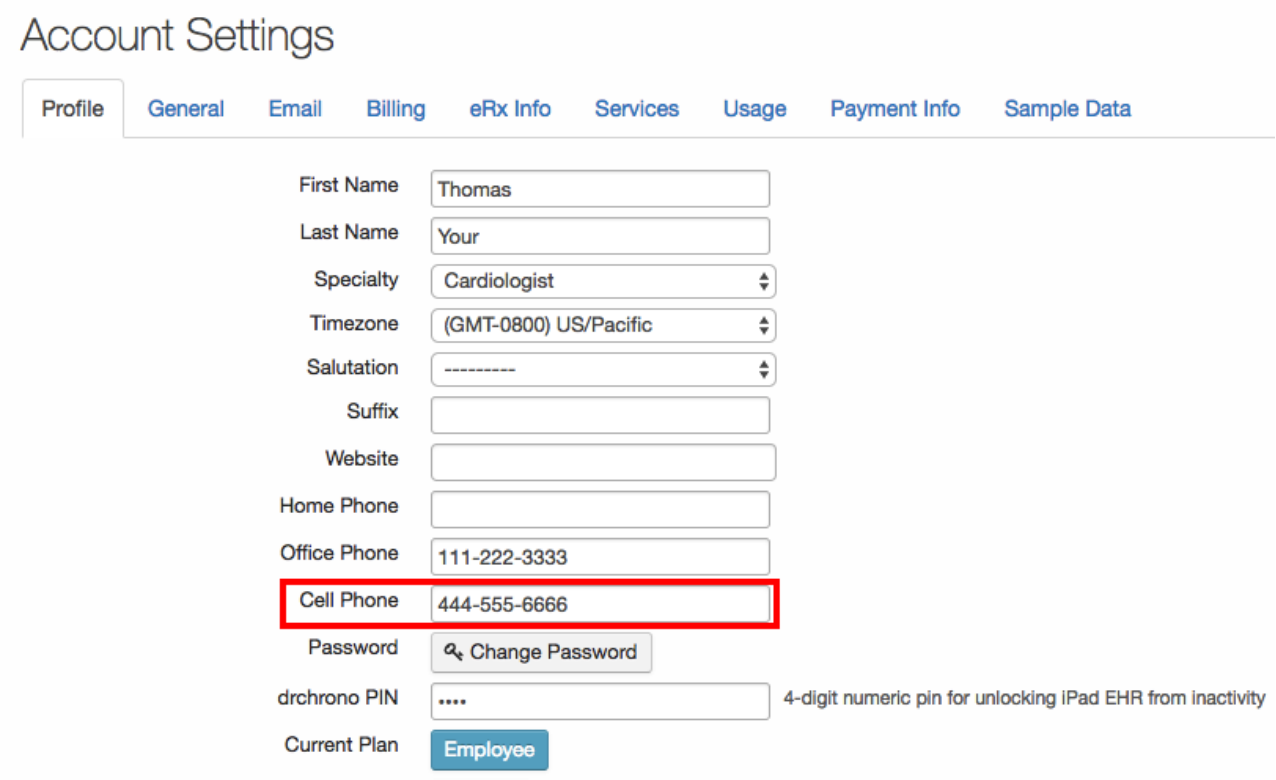
We've partnered with Authy to provide Two-Factor Authentication in DrChrono. When you create an account in DrChrono, an Authy account will also be created and linked to your DrChrono account. With our Authy integration, you have two options for 2FA.

- A rotating authentication code via the free Authy app synced with your DrChrono account (Recommended, more secure)
- Non-expiring authentication code via SMS (Not recommended, less secure).

1. To set up 2FA, go to **Account** > **Provider Settings**.

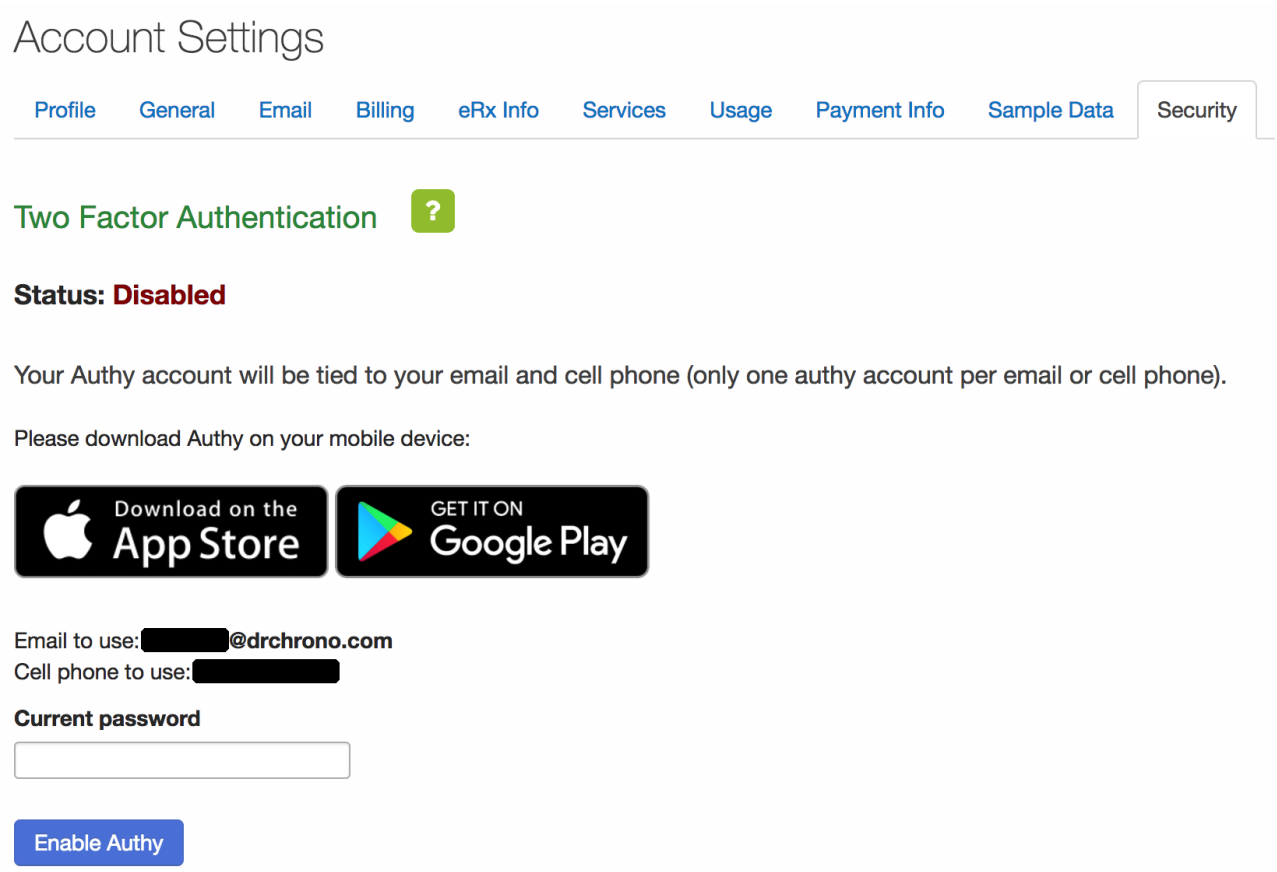


2. In your account settings, ensure you have a cell phone number entered in the **Profile** tab. If you do not have a number entered, type in your cell phone number.



3. Click **Update Entire Profile** at the bottom of the page.

4. To set up 2FA, select the Security tab. Your email address and cell phone will be displayed in the fields below according to the information you entered on the 'Profile' tab. Verify this information, type in your **DrChrono password**, and select **Enable Authy**.

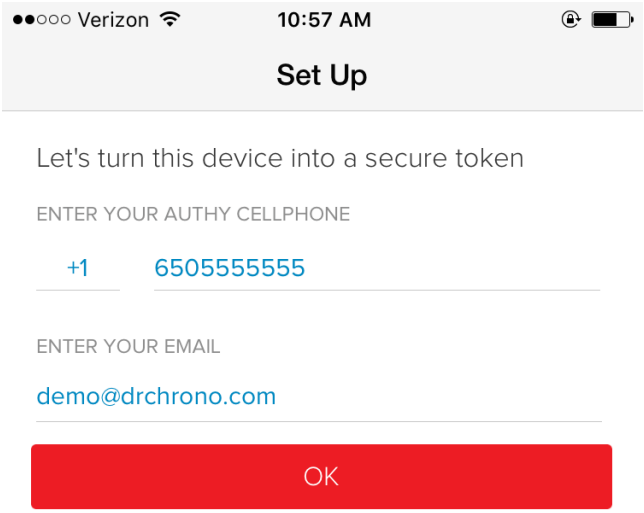


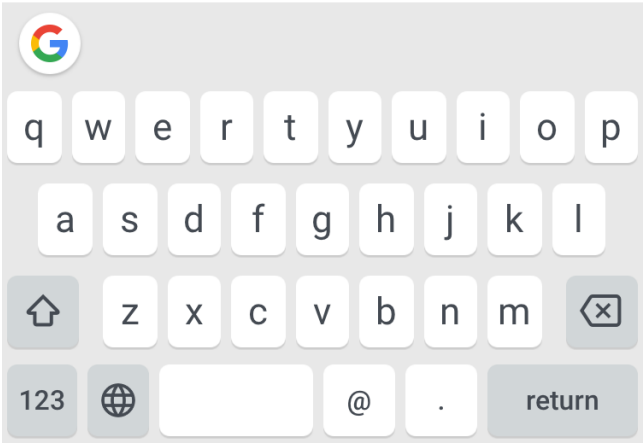
5. At this point, 2FA will be enabled on your account but configured to receive non-expiring authorization tokens via SMS, which does not provide a high degree of security. **We highly recommend downloading the Authy app, which produces time-sensitive tokens.** Download the Authy app on your mobile device by clicking either the iOS App Store or Google Play Store buttons on the page.

Setting Up the Authy App

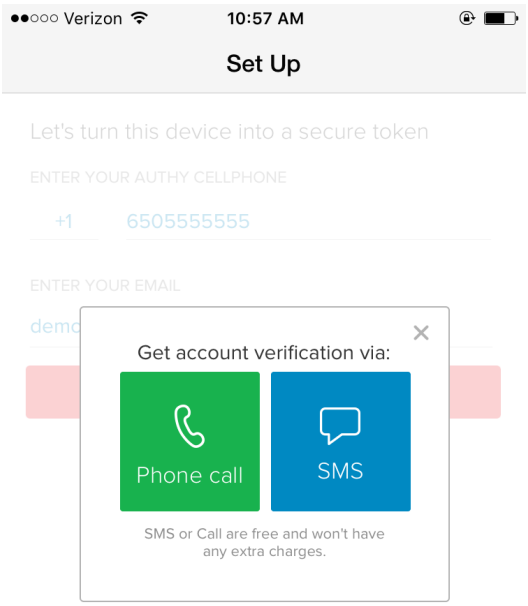
1. To set up Authy with DrChrono, open the Authy app on your mobile device.

2. In your Authy app, you'll be prompted to enter a phone number. Enter the cell phone number associated with your DrChrono account.

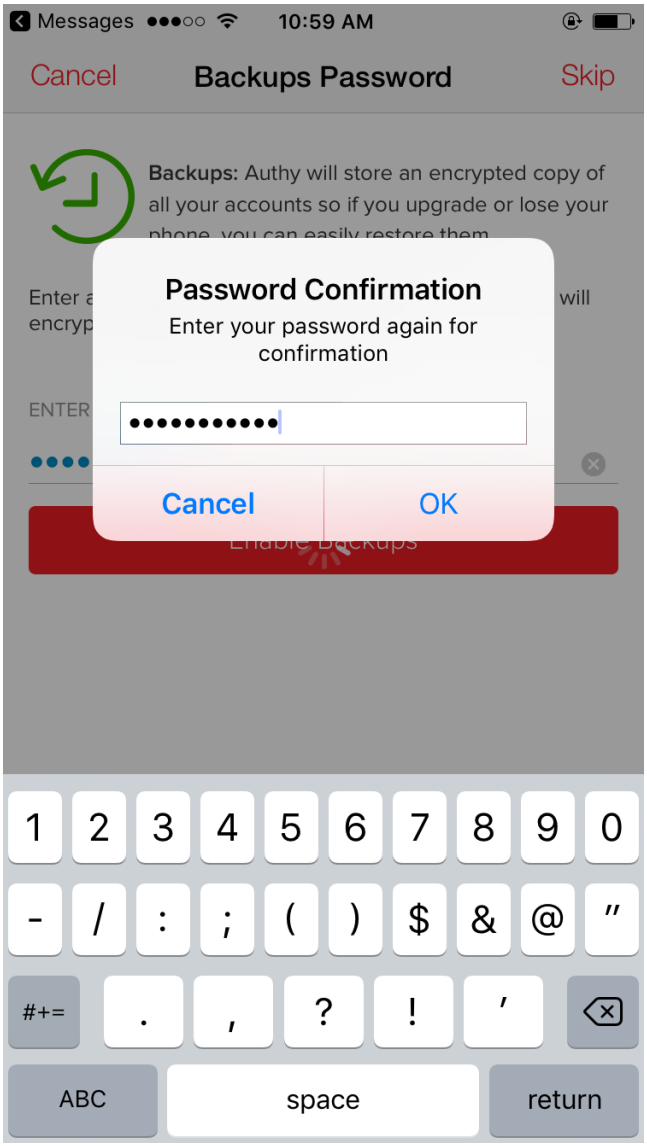




3. Authy will then ask you to verify your phone number via SMS or Phone Call. Select an option, and you will receive a verification code from Authy, which you may enter in the app. Once you verify your phone number, Authy will automatically search for your DrChrono account and sync your Authy app with DrChrono.

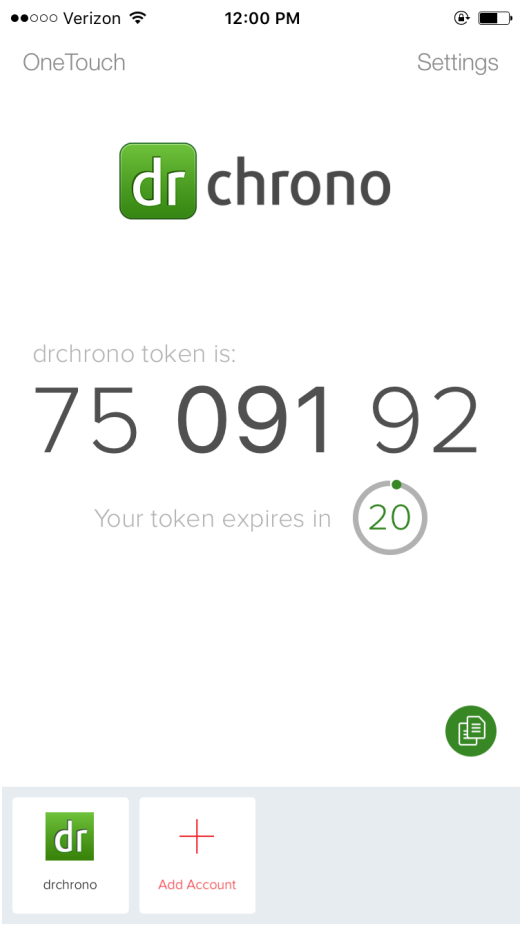


4. In the next step, you will be prompted to set up a backup password. We highly recommend this step to prevent lockouts in the event your phone is broken, lost, or stolen. Once you finish this step, the setup process will be completed. **This password is associated with your Authy account and does not need to be your DrChrono password.**



5. In your Authy app, you will now see DrChrono as one of your Authy accounts. When you select DrChrono from your list of accounts, a seven-digit code appears on the display. **When you log into DrChrono, you will be prompted for an authorization token. Enter this code to log in to your account.**

To see the log-in process in more detail, see our guide here: How does Two-Factor Authentication (2FA) work in DrChrono?


●●○○○ Verizon
12:00 PM
OneTouch
Settings
drchrono
drchrono token is:
75 091 92
Your token expires in
20
drchrono
Add Account