Set Up Two-Factor Authentication (2FA) for Staff

Last modified on 06/17/2026 12:57 am EDT

You can set up two-factor authentication (2FA) for staff on the **Staff** page.

Recommended practice roles

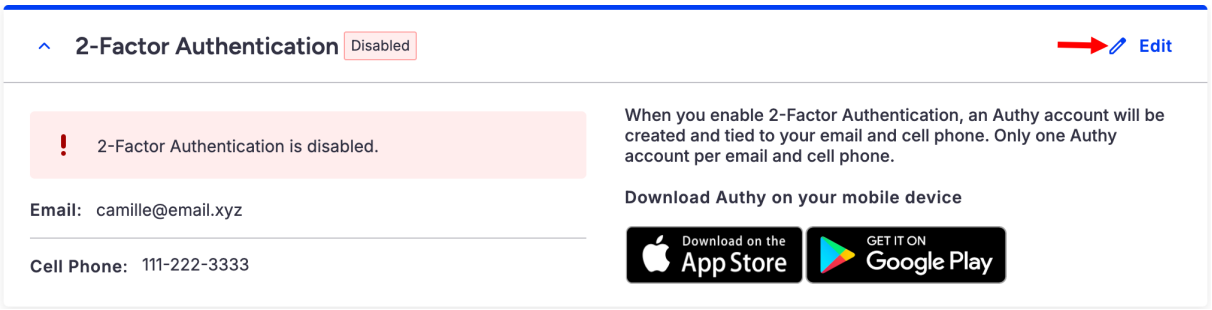
Practice administrators/office managers

Requirements

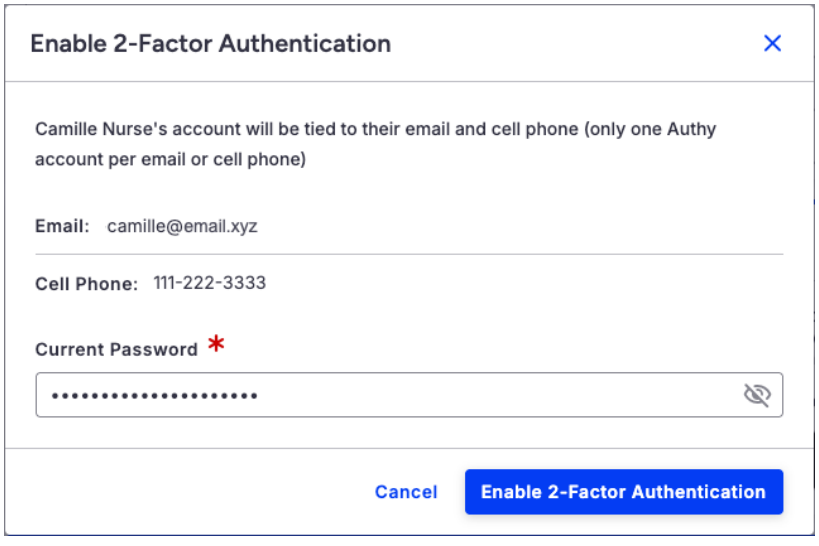
- Practice administrators or office managers must have the **Manage Accounts** permission turned on.
- Staff must have a cell phone number saved in their account set up.

Set up 2FA for a staff member

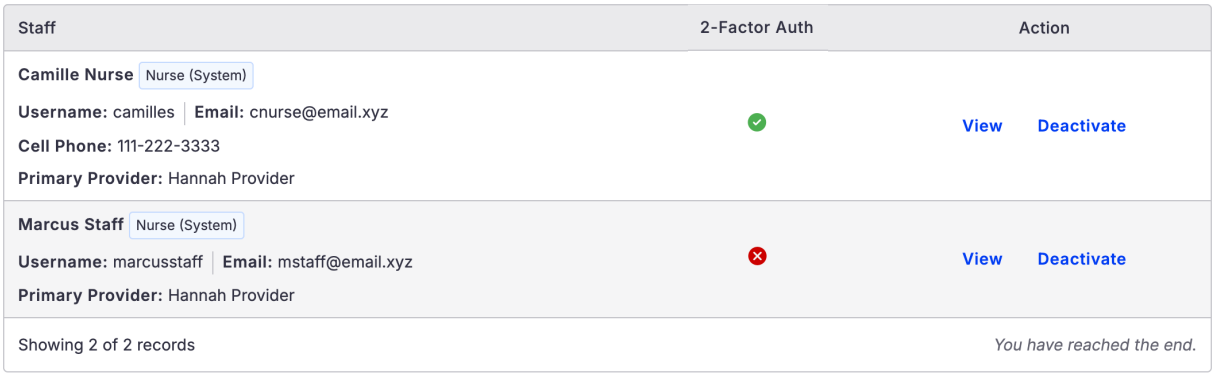
1. Select **Account** > **Practice Management** > **General Management** > **Staff**.
2. Select **View** for the specific staff member.
3. Scroll down to the **2-Factor Authentication** section and select **Edit** to open the **Enable 2-Factor Authentication** window.



4. Enter your password (not the staff member's password) and select **Enable 2-Factor Authentication**



On the **Staff** page, a green check mark shows under **2-Factor Auth**.



What happens after 2FA is turned on

Once you turn on 2FA for the staff member, an Authy account is created and tied to their email address and cell phone number.

> Only one Authy account is allowed per email or cell phone number.

The best practice is to have staff members set up the Authy app described in Set Up Two-Factor Authentication (2FA) for Your Account. The staff member must download the Authy app on their mobile device to complete authentication.

Staff member's first login with 2FA

Upon logging in to DrChrono, the staff member is prompted to enter a security code. They can do one of the following:

- Enter the security token from the Authy app and select **Log In**.
- Select **Request Token via SMS** to have the code is sent to their cell phone number, and then select **Log In**.