2FA - Two-factor authentication

> **Two-factor authentication (2FA), also known as multi-factor authentication (MFA) is mandatory for all Admin and Sub-admin accounts that do not have IP-based login restrictions.**

Setting Up Mandatory Two-Factor Authentication (2FA)

Two-factor authentication (2FA), also known as multi-factor authentication (MFA), adds an extra step to your basic login procedure. Without 2FA, the password is your single factor of authentication. With 2FA, you log in to the Admin Panel by entering your username and password and the six-digit code provided by an app installed on your smartphone.

Because this security measure is now mandatory for all accounts without IP restrictions, you will be prompted to enable 2FA for the account upon logging in, if it is not already active.

Enable 2FA for the Admin Panel

> If you're using this Admin account as credentials for the API, WHMCS, or similar integrations, the API login will fail after enabling 2FA. To solve this, create a Sub-Admin with special permissions for the API authentication only.
>
> **Click here for more details on secure API setup.**

Phase 1: Download an Authenticator App

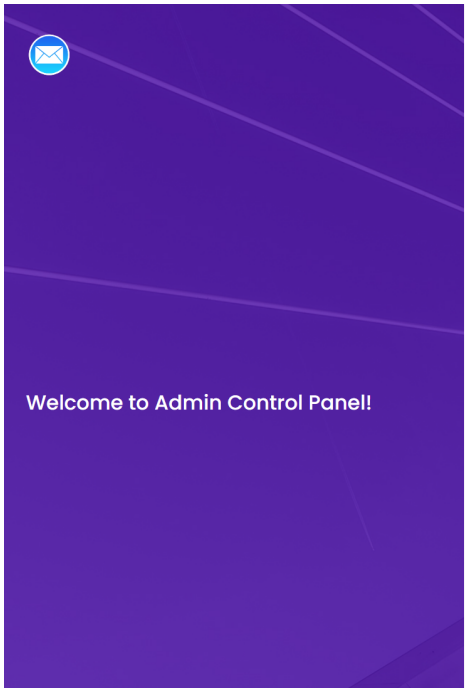
Before you can scan the barcode on your computer screen, you need the correct software on your mobile device. You must have a smartphone with a 2FA App installed, such as Authy or Google Authenticator.

1. Open the app store on your smartphone.
2. Search for and download a free authenticator app like Authy or Google Authenticator.
3. Open the app on your phone and look for an option to add a new account or scan a QR code.

Phase 2: Connect Your Account

Once the app is ready on your phone, return to your computer screen to complete the enrollment.

1. Locate the square barcode, known as a QR code, displayed on your **Admin Panel** setup page.
2. Scan the QR code with the installed 2FA App. Point your smartphone camera at the computer screen.
3. Look at your smartphone screen. The app will generate a six-digit code.
4. Fill in the generated **six-digit code** in the **Your code** input field from the Admin Panel.





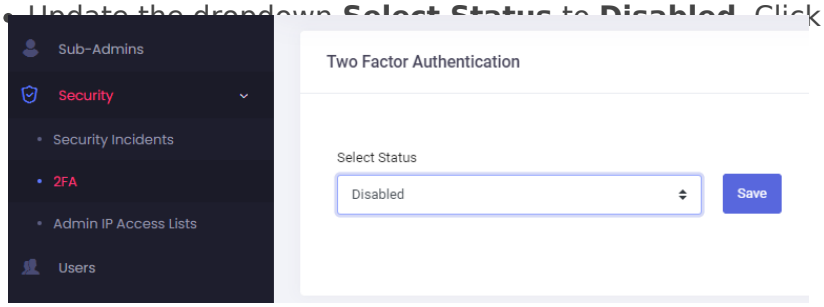
5. Click on the **Verify and continue** button before your token expires. The numbers in your authenticator app refresh automatically every 30 seconds.

Disable 2FA for the Admin Panel

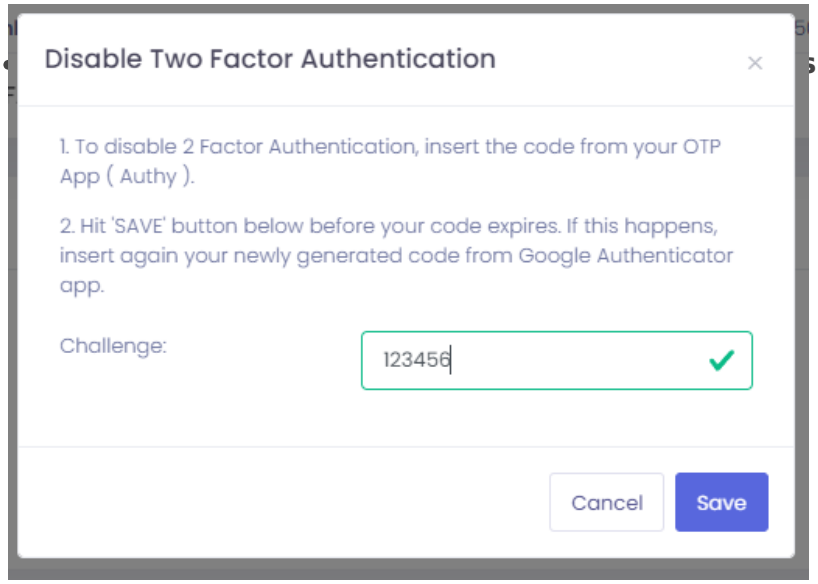
> You can only disable 2FA if your Admin login is restricted to specific IP addresses. If your login access remains unrestricted, 2FA is mandatory and cannot be disabled.
>
> Before proceeding, please ensure you have configured your IP restrictions. You can learn how to do this in our guide on Restricting Login Access via Admin IP Access Lists.

To disable the 2FA for your Admin account:

- Log in to the **Admin Panel**
- From the menu, go to **Security → 2FA**
- Update the dropdown **Select Status** to **Disabled**. Click on the **Save** button.



- Insert the token from your 2FA App (such as Authy or Google Authenticator) in the



- After you see the confirmation message that the 2FA was disabled, you can delete the entry from your 2FA app.

Revision #5
Created 24 August 2024 11:09:57 by Support
Updated 29 October 2026 19:29:37 by Admin