Two-Factor Authentication for WHM

(*WHM >> Home >> Security >> Two-Factor Authentication*)

Overview

This function allows you to configure two-factor authentication (2FA), an improved security measure for the login interface of cPanel & WHM. Two-factor authentication requires two forms of identification:

- Your password
- A generated security code

When you enable 2FA, an application on your smartphone supplies a code that you **must** enter with your password to log in. Without your smartphone, you cannot log in. For more information about 2FA, read Wikipedia's Two-Factor Authentication article.

Important:
If you or your users see a *Failed to set user configuration: The security code is invalid.* error, a problem may exist with the date and time settings on your server.

- To fix the issue, use the `ntpdate` command to re-synchronize your server's internal clock with the Network Time Protocol (NTP) server.
- 2FA **requires** an accurate server time in order to function properly.

Note:
2FA **requires** a smartphone with a supported time-based one-time password (TOTP) app. We suggest the following apps:

- For Android™, iOS®, and Blackberry® — Google Authenticator™
- For Android and iOS — Duo Mobile
- For Windows® Phone — Authenticator

Enable 2FA

Warning:
This feature may cause some third-party applications to break significantly, and may cause applications to improperly store data.

If 2FA is disabled on the server, click the toggle to change it to *On* and enable 2FA.

Note:
Only the `root` user can enable 2FA.

Settings Manage Users Manage My Account

Settings

The *Settings* tab allows you to configure the 2FA *Issuer* setting. The *Issuer* setting determines the name that appears in the authentication app when a user accesses the security code.

To customize the *Issuer* setting for 2FA, perform the following steps:

1. Click the *Settings* tab.
2. Enter the desired value for the *Issuer* setting, or retain the default value.

Note:
If you do not enter a name for the *Issuer* setting, it defaults to the hostname.

3. Click *Save*.

Manage Users

The *Manage Users* tab displays the accounts for which you have configured 2FA, and allows you to disable 2FA on those accounts.

Remove 2FA on a user account

To remove 2FA for a single user account on the *Manage Users* list, click *Disable* to the right of the user account.

To remove multiple user accounts from the *Manage Users* list, perform the following steps:

1. Select the *Manage Users* tab.
2. Select the checkboxes to the left of each user account that you want to remove, or select the checkbox to the left of the *User* heading to select them all.
3. Click the gear icon (

) on the top right of the list, and then select *Disable Selected*.

Note:
Select *Disable All* to remove every user account from the *Manage Users* list. This will **not** disable 2FA on your own account.

Enable 2FA on a user account

Important:
You **cannot** enable 2FA for a user account through the WHM interface. However, you **must** enable the *Two-Factor Authentication Security Policy* on the server in order to enable 2FA for cPanel accounts.

To enable 2FA for a user account, log in to the cPanel interface as the user and navigate to cPanel's *Two-Factor Authentication* interface (*cPanel >> Home >> Security >> Two-Factor Authentication*).

Alternatively, you can call API functions to access 2FA functionality. For more information, read our Guide to API Authentication documentation.

Manage My Account

The *Manage My Account* tab allows you to set up 2FA for the `root` account or a reseller account.

Important:
To use Two Factor Authentication in WHM, the reseller account **must** possess the *Create Accounts* (`create-acct`) privilege in WHM's *Edit Reseller Nameservers and Privileges* interface (*WHM >> Home >> Resellers >> Edit Reseller Nameservers and Privileges*) .

Configure 2FA

To configure 2FA, perform the following steps:

1. Click *Set Up Two-Factor Authentication.*
2. To configure 2FA, you **must** create a link between your cPanel account and your 2FA app:
    - To automatically create the link, scan the displayed QR code with your app.
    - To manually create the link, enter the provided *Account* and *Key* information in your app.
3. Within your 2FA app, retrieve the six-digit security code.

> **Note:**
> The 2FA app generates a new six-digit security code for your cPanel account every 30 seconds.

4. Enter the six-digit security code in the *Security Code* text box.

> **Note:**
> You **must** enter the security code within 30 seconds. After time expires, the app will generate a new six-digit code.

5. Click *Configure Two-Factor Authentication*.

Remove 2FA

To remove 2FA, click *Remove Two-Factor Authentication*.

Reconfigure 2FA

To reconfigure 2FA, click *Reconfigure*. Then, follow the steps to configure 2FA.

> **Warning:**
> If you reconfigure 2FA for your account, any existing configurations will no longer produce valid security codes.

Additional documentation

Suggested documentation For cPanel users For WHM users For developers

- Two-Factor Authentication for WHM
- Configure Security Policies
- Manage Wheel Group Users
- Manage External Authentications
- The failurls File

- Two-Factor Authentication for cPanel
- SSH Access
- SSL TLS Wizard
- Security Policy
- ModSecurity

- Two-Factor Authentication for WHM
- Configure Security Policies
- Basic Security Concepts
- Manage Wheel Group Users
- Manage External Authentications

- Guide to API Authentication - API Tokens in WHM
- UAPI Functions - TwoFactorAuth::remove_user_configuration
- UAPI Functions - TwoFactorAuth::set_user_configuration

- UAPI Functions - TwoFactorAuth::generate_user_configuration
- UAPI Functions - TwoFactorAuth::get_user_configuration