More Ways to Secure Your WHMCS Installation

Your WHMCS installation will store sensitive information for your customers and for your business. We take steps as we develop each WHMCS version to help ensure a secure system. However, to go even further in protecting against security issues, we recommend taking a series of additional steps to secure your installation.

> ❗ The steps below provide extra protection against hackers and other malicious attackers. If you have questions about security, contact your hosting provider or system administrator.

To enhance the protection of your WHMCS installation, we recommend that you:

1. Secure your installation's writeable directories.

We recommend moving all writeable directories to a private location in order to prevent web-based access. When you do this, you must also make necessary changes to your file storage settings and the templates cache.

For steps to do this, see Securing Writeable Directories.

2. Secure the configuration.php file.

We recommend adjusting the permissions for the `configuration.php` file in your WHMCS root directory. This file contains sensitive data that you can't recover without a backup copy of the file.

Changing the file permissions helps to avoid accidentally overwriting, editing, or deleting the file.

For steps to do this, see Securing the Configuration File.

3. Move the crons directory.

We recommend moving the `crons` directory to a private directory above your web root. This will prevent web-based access and help to protect your WHMCS installation.

For steps to do this, see Moving the Crons Directory.

4. Restrict access to your WHMCS installation's Admin Area.

For increased protection, if your staff uses fixed IP addresses, you can restrict access to a specific set of IP addresses. This will help to prevent access by hackers and other malicious users.

For steps to do this, see Restricting Access by IP Address.

5. Rename the WHMCS Admin Area directory.

Customizing the name of your WHMCS `admin` directory makes it harder for bots and other malicious users to find the login URL for your WHMCS Admin Area.

For steps to do this, see Renaming the WHMCS Admin Directory.

6. Enable SSL for your domain.

WHMCS often contains private and sensitive data that passes between WHMCS and end users' browsers. Having a valid SSL certificate that enables the use of HTTPS and encrypted communication is essential for data security.

For steps to do this, see Enabling SSL.

7. Restrict the WHMCS database's privileges.

We recommend disabling any unneeded database privileges. WHMCS requires a specific set of permissions for day-to-day use and additional privileges during installation, upgrades, and module activations.

For more information and lists of the required permissions, see Database Privileges.

8. Prohibit serving requests directly from the vendor directory.

The `vendor` directory includes various common libraries that WHMCS uses. To prevent unexpected behavior and other issues, your server should not serve file requests directly from this path.

If your server runs Apache, the included `.htaccess` file already protects against these problems. If, however, you use a different web server technology, you will need to update your configuration to prohibit serving files directly from the `vendor` directory.

For steps to do this with NGINX, see Nginx Directory Access Restriction.

9. Defend against clickjacking.

In a clickjacking attack, the attacker loads an external page (like the WHMCS Client Area) and attempts to trick the user into granting access to their information. You can prevent this by ensuring that your site always sends the proper Content Security Policy (CSP) frame-ancestors directive response headers.

For steps to do this, see OWASP Clickjacking.

10. Take general server hardening steps.

The additional steps that you can take depend on your hosting control panel and server configuration. For example:

- cPanel's Security Best Practices
- OWASP Security Misconfiguration