

ModSecurity Vendors

This document is for a previous release of cPanel & WHM. To view our latest documentation, visit our [Home page](#).

For cPanel & WHM 11.48

([Home](#) >> [Security Center](#) >> [ModSecurity™ Vendors](#))

Overview

The *ModSecurity™ Vendors* interface allows you to install and manage your ModSecurity vendors.

Important:

You **must** install the ModSecurity Apache module in order to use this feature. To install the ModSecurity Apache module, use WHM's *EasyApache (Apache Update)* interface ([Home](#) >> [Software](#) >> *EasyApache (Apache Update)*).

Note:

The system loads the `/usr/local/apache/conf/modsec2.user.conf` file as an include.

- In previous versions of cPanel & WHM, EasyApache used this file as the default ruleset.
- This file's rules may still affect the way in which ModSecurity functions, which may result in false positives on your system.
- If you see many false positives, check this file for custom rules.

Add a ModSecurity vendor

To add a ModSecurity™ vendor, perform the following steps:

1. Click *Add Vendor*.
2. In the *Vendor Configuration URL* text box, enter the URL for the ModSecurity vendor.
3. Click *Load*. The *Vendor Name*, *Vendor Description*, *Vendor Documentation URL*, and *Vendor Path* text boxes automatically load vendor data.
4. After you confirm that the vendor data is correct, click *Save*.

Notes:

- To add a vendor in a disabled state, deselect the *Enabled* checkbox.
- When you add a vendor, the interface prompts you to enable or disable each of the vendor's configuration files. You **must** enable the vendor's configuration files in order to use the vendor's rules.

Manage Vendors

Note:

To manage these functions from the command line, run the following script as the `root` user:

```
/usr/local/cpanel/scripts/modsec_vendor
```

Install a ModSecurity vendor

To install a cPanel-provided ModSecurity vendor, click *Install* for that vendor, and then click *Install and Restart Apache*.

Enable or disable a vendor

- To enable a vendor, click *On* in the *Enabled* column for that vendor.
- To disable a vendor, click *Off* in the *Enabled* column for that vendor.

Enable or disable updates

When you enable updates, the system retrieves new copies of the vendor metadata from the URL that you used during vendor installation. The system compares the downloaded metadata and automatically fetches and installs new versions of the rule set.

- To enable automatic updates for a vendor, click *On* in the *Updates* column.
- To disable automatic updates for a vendor, click *Off* in the *Updates* column.

Note:

The system checks for vendor updates when the `/scripts/upcp` script runs. For more information, read our [How to Update Your System](#) and [Update Preferences](#) documentation.

Edit a vendor

The ModSecurity vendor rule sets group common rules into separate configuration files. To selectively enable or disable the configuration files, edit the vendor.

To edit a ModSecurity vendor, perform the following steps:

1. Click *Edit* for the vendor that you wish to edit.
2. Click *Enable All*, click *Disable All*, or click the toggle to enable or disable each configuration file.

Delete a vendor

To delete a ModSecurity vendor, locate the vendor in the list, click *Delete*, and then click *Delete*.