ModSecurity Tools

This documentation is for cPanel & WHM version 70 CURRENT builds. The "RELEASE" version of our documentation can be found in the Version 68 Documentation space.

(*WHM >> Home >> Security Center >> ModSecurity™ Tools*)

Overview

The *ModSecurity™ Tools* interface allows you to install and manage ModSecurity rules.

- Click *Rules List* to view the *Rules List* section of the interface.
- In the *Rules List* section of the interface, click *Hits List* to return to the *Hits List* section of the interface.

Important:
You **must** install the ModSecurity Apache module in order to use this interface.

- If your system runs EasyApache 3, use WHM's *EasyApache 3* interface *(WHM >> Home >> Software >> EasyApache 3*) to install the ModSecurity Apache module.
- If your system runs EasyApache 4, use WHM's *EasyApache 4* interface (*WHM >> Home >> Software >> EasyApache 4*) or the `yum install ea-apache24-mod_security2` command to install the ModSecurity Apache module.

Note:
If your system runs EasyApache 3, the system loads the `/usr/local/apache/conf/modsec2.user.conf` file as an include. EasyApache 4 loads the `/etc/apache2/conf.d/modsec/modsec2.cpanel.conf` and `/etc/apache2/conf.d/modsec/modsec2.user.conf` files as an include.

- 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.

Hits List

Use the *Hits List* section of the interface to view your server's history of rule events. To edit or disable the ModSecurity rule that generated a hit, click *Rule ID*.

Report a rule

If you find a problem with a vendor's rule, perform the following steps to report the issue to the rule's vendor:

1. Locate the hit that the rule generated in the *Hits List* and click *More*.
2. Click *Report this hit.*

   Note:
   This option does **not** appear if the vendor does not accept reports.

3. Enter your email address, the reason for the report, and any additional comments for the vendor.
4. Click *Review Report*.
5. Verify the information in your report and click *Submit*.

Rules List

Important:
To update the Apache server with your staged changes, click *Deploy and Restart Apache* at the top or bottom of the interface.

Note:
For more information about how to create your own ModSecurity rules, read GitHub's ModSecurity Reference Manual documentation.

Filter rules

To filter the list of rules, click the *Vendor* button in the right corner of the table. Click the vendors that you wish to display in the *Vendors* menu and click *Apply*. To deselect a vendor, hold the *Control* key while you click the vendor.

Add a rule

To add a rule, perform the following steps:

1. Click *Add Rule*. A new interface will display.
2. Enter the rule in the *Rule Text* text box.
3. To enable the rule when you deploy the configuration, select the *Enable Rule* checkbox.
4. To deploy the rule and restart Apache immediately, select the *Deploy and Restart Apache* checkbox.
5. Click *Save*.

Edit a rule

To edit a rule, perform the following steps:

1. Click *Edit* for the rule that you wish to update.
2. Make the desired changes in the *Rule Text* text box.
3. Click *Save.*

> **Note:**
> You **cannot** edit vendor rules. To remove all of a vendor's rules from your system, use the *ModSecurity Vendors* interface (*WHM >> Home >> Security Center >> ModSecurity™ Vendors*).

Copy a rule

To copy a rule, perform the following steps:

1. Click *Copy* for the rule that you wish to update.
2. Make any desired changes in the *Rule Text* text box.
3. Click *Save*.

Edit all rules

To edit all of your rules, perform the following steps.

1. Click *Edit Rules*.
2. Enter the desired changes in the *Rules* text box.
3. Click *Save*.

> **Remember:**
> You **cannot** edit vendor rules. To remove all of a vendor's rules from your system, use the *ModSecurity Vendors* interface (*WHM >> Home >> Security Center >> ModSecurity™ Vendors*).

Enable or disable a rule

To enable or disable a ModSecurity rule, click *Enable* or *Disable* in that rule's row.

Delete a rule

To delete a rule, perform the following steps:

1. Click *Delete* for the rule that you wish to delete.
2. Click *Delete* to confirm your action.

> **Note:**

You **cannot** delete vendor rules. To remove all of a vendor's rules from your system, use the *ModSecurity Vendors* interface (*WHM >> Home >> Security Center >> ModSecurity™ Vendors*).

ModSecurity database script

To create the ModSecurity database manually, run the following command:

```
/usr/local/cpanel/scripts/setup_modsec_db
```

Additional documentation

Suggested documentation For cPanel users For WHM users For developers

- ModSecurity Tools
- ModSecurity Vendors
- ModSecurity Configuration
- cPHulk Brute Force Protection
- Manage Service SSL Certificates

- ModSecurity
- Security Policy
- Manage Certificate Sharing
- Directory Privacy
- SSH Access

- ModSecurity Tools
- ModSecurity Vendors
- How to Create a Report Receiver API for the ModSecurity Rule Reports
- OWASP ModSecurity CRS
- How to Create a ModSecurity Vendor

- WHM API 1 Functions - modsec_get_vendors
- WHM API 1 Functions - modsec_add_vendor
- WHM API 1 Functions - modsec_remove_vendor
- WHM API 1 Functions - modsec_preview_vendor
- WHM API 1 Functions - modsec_enable_vendor