

**Web Application Firewall**  
POWERED BY **COMODO**

# Comodo Web Application Firewall for cPanel

Software Version 2.11

## Administrator Guide

Guide Version 2.11.120318

## Table of Contents

<b>1. Comodo Free ModSecurity Rules for cPanel - Introduction.....</b>	<b>3</b>
1.1. System Requirements.....	3
<b>2. Deploying Comodo ModSecurity Rule Set in cPanel.....</b>	<b>3</b>
<b>About Comodo Security Solutions.....</b>	<b>8</b>

# 1. Comodo Free ModSecurity Rules for cPanel - Introduction

This guide explains how server administrators can use cPanel to download, implement and manage Comodo Mod-Security rule sets.

Once installed and configured, CWAF just requires the latest firewall rule sets to be downloaded and deployed to your servers. The simple web administration console allows administrators to manually download and implement the latest rule set or a rule-set from a previous version. Administrators can install the CWAF agent or the web hosting control panel plugin (currently cPanel, DirectAdmin and Plesk plugins are available) to automatically fetch and install the new rules as soon as they become available. The plugins can also be used to configure the overall behavior of CWAF and to customize the rule sets by excluding unwanted rules from implementation.

CWAF has been tested on Apache and LiteSpeed on Linux servers. Versions for other web-server types are coming shortly.

CWAF is also integrated as a ModSecurity vendor in cPanel, DirectAdmin and Plesk panels and users can enable/disable Comodo protection rules and manage them with panel's internal tools.

## Guide Structure

This guide is intended to take the administrator through the setup, configuration and use of Comodo Web Application Firewall in cPanel.

- **Comodo Web Application Firewall - Introduction** - A high level description of the product
- **System Requirements** - List of compatible server environments for CWAF
- **Deploying Comodo ModSecurity Rule Sets in cPanel** - Guidance on downloading and deploying the firewall rule sets on to the server

## 1.1. System Requirements

The Web Application Firewall can be implemented on to the following web application servers:

- Apache or LiteSpeed web server on Linux server platform
- ModSecurity 2.7.5 and higher

# 2. Deploying Comodo ModSecurity Rule Set in cPanel

Comodo ModSecurity protection rules are now integrated in cPanel and can be activated from the 'Security Center'.

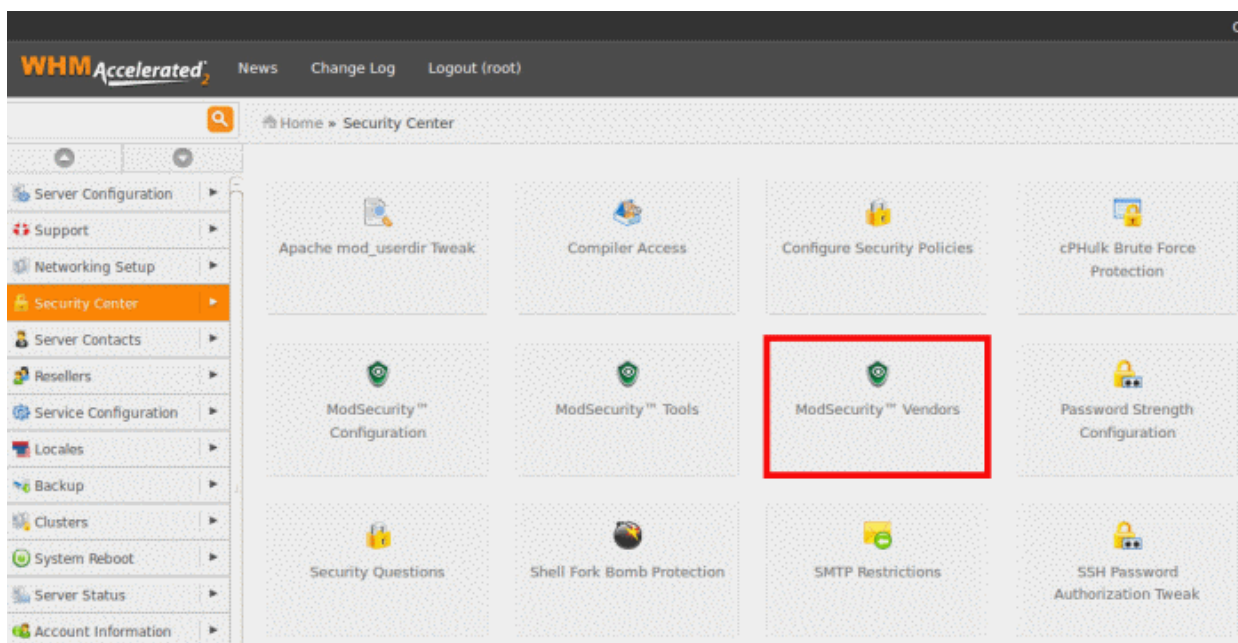
- Sign in to your cPanel account



The image shows the WHM login interface. At the top, the 'WHM' logo is displayed in large orange letters. Below the logo, there are two input fields: one for 'Username' with a placeholder 'Enter your username.' and one for 'Password' with a placeholder 'Enter your account password.' and a lock icon. At the bottom of the form is an orange 'Log in' button.

**Important Note:** cPanel ModSecurity Vendors are not compatible with CWAF plugin. So, you can't use both in parallel for management of your protection rules.  
Don't activate both Comodo Rule Sets for Apache and LiteSpeed simultaneously to avoid conflicts.

- Click the 'Security Center' tab from the left menu, then 'ModSecurity Vendors'



- Click 'Add Vendor' in the 'ModSecurity Vendor Manager' screen.

Home » Security Center » Manage Vendors

## ModSecurity™ Vendor Manager

Manage Vendors Add Vendor

Search

Page Size  First  Last

Vendor	Provider	Enabled ▲	Updates	Sets Included
OWASP ModSecurity Core Rule Set <a href="#">↗</a> SpiderLabs OWASP curated ModSecurity rule set		<input type="checkbox"/>	<input type="button" value="i"/> This vendor is not installed.	<input type="button" value="+ Install"/>

[Back To Top](#)

Page Size  First  Last

In the 'Add Vendor' page, enter the vendor configuration URL depending on your web server type.

- For Comodo ModSecurity Apache Rule Set - [https://waf.comodo.com/doc/meta\\_comodo\\_apache.yaml](https://waf.comodo.com/doc/meta_comodo_apache.yaml)
- For Comodo ModSecurity LiteSpeed Rule Set - [https://waf.comodo.com/doc/meta\\_comodo\\_litespeed.yaml](https://waf.comodo.com/doc/meta_comodo_litespeed.yaml)

### ModSecurity™ Vendor Manager

#### Add Vendor

Use this interface to add a Vendor for ModSecurity.

**Vendor Configuration URL**

The file name should begin with meta\_, followed by the short vendor identification code, and finally the .yaml extension.  
**Example:** https://example.com/example/meta\_example.yaml

**Vendor Name**

**Vendor Description**

**Vendor Documentation URL**

**Vendor Report URL**

**Path**

- Enter the appropriate URL in the 'Vendor Configuration URL' field and click 'Load' The vendor details will be fetched and automatically filled in the fields.
- Click the 'Save' button.

ModSecurity™ Vendor Manager

Manage Vendors Add Vendor

**Success:** You have successfully added \*COMODO ModSecurity Apache Rule Set\* to the vendor configuration list. x

Search Q Page Size 10 First 1 Last

Vendor	Provider	Enabled ▲	Updates	Sets Included
<a href="#">OWASP ModSecurity Core Rule Set</a> SpiderLabs OWASP curated ModSecurity rule set		<input type="checkbox"/>	<input type="checkbox"/> This vendor is not installed.	<a href="#">+ Install</a>
<b>COMODO ModSecurity Apache Rule Set</b> COMODO ModSecurity Rules for Apache	Third Party	<input checked="" type="checkbox"/> On <input type="checkbox"/> Off	<input checked="" type="checkbox"/> On <input type="checkbox"/> Off	8 / 8 <a href="#">Edit</a> <a href="#">Delete</a>

[Back To Top](#) Add Vendor Page Size 10 First 1 Last

That's it. Comodo ModSecurity Rules Set is now activated in cPanel.

# About Comodo Security Solutions

Comodo Security Solutions is a global innovator of cybersecurity solutions, protecting critical information across the digital landscape. Comodo provides complete, end-to-end security solutions across the boundary, internal network and endpoint with innovative technologies solving the most advanced malware threats. With over 80 million installations of its threat prevention products, Comodo provides an extensive suite of endpoint, website and network security products for MSPs, enterprises and consumers.

Continual innovation and a commitment to reversing the growth of zero-day malware, ransomware, data-breaches and internet-crime distinguish Comodo Security Solutions as a vital player in today's enterprise and home security markets.

## About Comodo Cybersecurity

In a world where preventing all cyberattacks is impossible, Comodo Cybersecurity delivers an innovative cybersecurity platform that renders threats useless, across the LAN, web and cloud. The Comodo Cybersecurity platform enables customers to protect their systems and data against even military-grade threats, including zero-day attacks. Based in Clifton, New Jersey, Comodo Cybersecurity has a 20-year history of protecting the most sensitive data for both businesses and consumers globally. For more information, visit [comodo.com](https://www.comodo.com) or our [blog](#). You can also follow us on [Twitter](#) (@ComodoDesktop) or [LinkedIn](#).

1255 Broad Street

Clifton, NJ 07013

United States

Tel : +1.877.712.1309

Tel : +1.888.551.1531

<https://www.comodo.com>

Email: [EnterpriseSolutions@Comodo.com](mailto:EnterpriseSolutions@Comodo.com)