

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

# Comodo Web Application Firewall for DirectAdmin

Software Version 2.11

## Administrator Guide

Guide Version 2.11.120418

## Table of Contents

<b>1. Comodo Free ModSecurity Rules for DirectAdmin - Introduction.....</b>	<b>3</b>
1.1. System Requirements.....	3
<b>2. Deploying Comodo ModSecurity Rule Set in DirectAdmin.....</b>	<b>3</b>
2.1. Using the CWF Plugin for Firewall Configuration.....	6
<b>About Comodo Security Solutions.....</b>	<b>8</b>

# 1. Comodo Free ModSecurity Rules for DirectAdmin - Introduction

This guide explains how server administrators can use DirectAdmin to download, implement and manage Comodo ModSecurity 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, Plesk plugins and Webmin 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 and Nginx on Linux servers.

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 DirectAdmin panel

- **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 DirectAdmin** - Guidance on downloading and deploying the firewall rule sets on to the server
- **Using the CWAF Plugin for Firewall Configuration** - Guidance on using the CWAF plugin for downloading and deploying the firewall rule sets

## 1.1. System Requirements

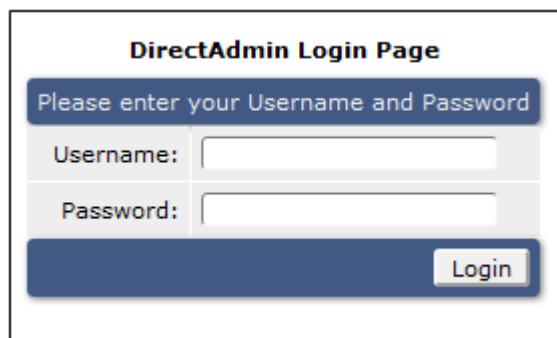
The Web Application Firewall can be implemented on to the following web application servers:

- Apache 2 and higher web server on CentOS, Debian and FreeBSD server platform
- ModSecurity 2.7.5 and higher

# 2. Deploying Comodo ModSecurity Rule Set in DirectAdmin

Comodo ModSecurity protection rules are now integrated in DirectAdmin panel and can be activated from the 'CustomBuild' feature.

- Sign in to your DirectAdmin account



The image shows a login form titled "DirectAdmin Login Page". It contains a blue header bar with the text "Please enter your Username and Password". Below this are two input fields: "Username:" and "Password:". At the bottom right of the form is a "Login" button.

The DirectAdmin home page will be displayed.

- Make sure CPAN and SUDO utilities are installed on your system.
- Click on 'CustomBuild' link under the 'Extra Features' section.

Please make sure that you have the latest 'CustomBuild' version. For more information about DirectAdmin CustomBuild, refer to the forum page at <http://forum.directadmin.com/showthread.php?t=44743>



- Click the 'Update' button in the 'CustomBuild' interface.

Update Software | Build Software | Edit Options | Update Software Configuration | Remove Software | CustomBuild Functions

Customize Compilation | Customize Versions | Plugin Logs

---

**DirectAdmin**

DirectAdmin 1.47.0 update to 1.48.3 is available [Update](#)

**Comodo ModSecurity Rule Set**

Comodo ModSecurity Rule Set 1.03 update to 1.12 is available [Update](#)

**Pure-FTPd**

Pure-FTPd 1.0.37 update to 1.0.41 is available [Update](#)

**Libpng**

Libpng 1.6.16 update to 1.6.17 is available [Update](#)

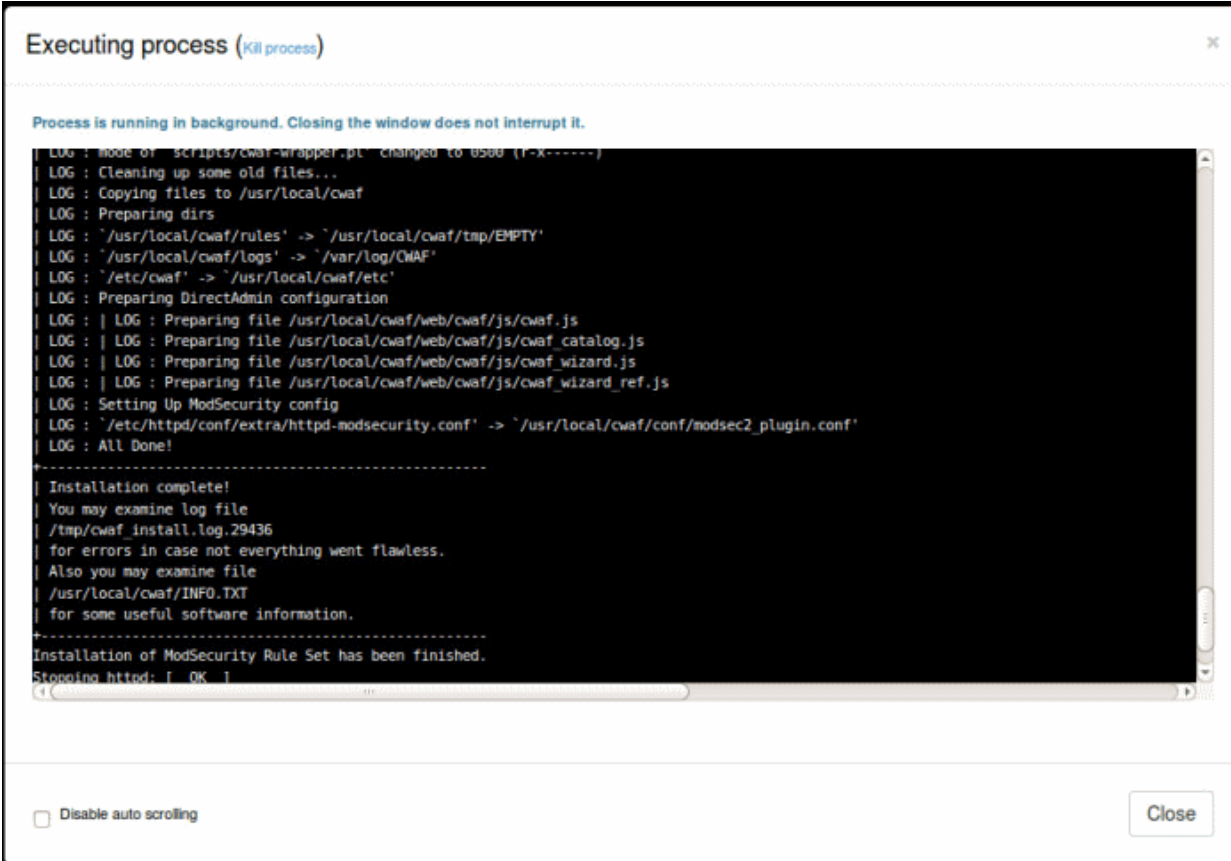
[Update all](#)

© 2014 Martynas Bendorius, MB Martynas IT, [martynas.it](http://martynas.it)  
Page load time: 1.0579 seconds

MARTYNAS IT  
PROFESSIONAL SERVER MANAGEMENT

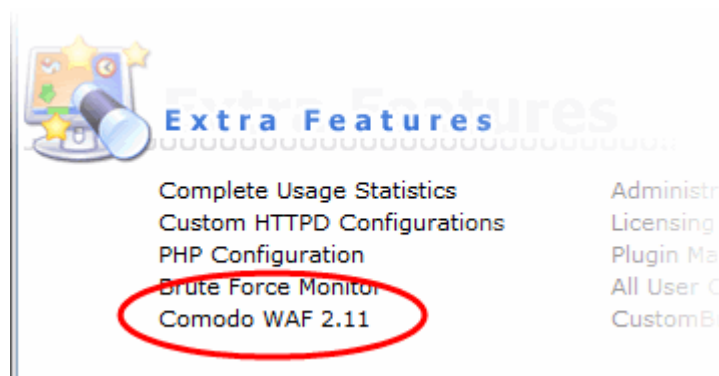
admin > Plugins

The installation processes will be displayed...



```
Executing process (Kill process)
Process is running in background. Closing the window does not interrupt it.
LOG : mode of scripts/cwaf-wrapper.pl changed to 0500 (r-x-----)
LOG : Cleaning up some old files...
LOG : Copying files to /usr/local/cwaf
LOG : Preparing dirs
LOG : /usr/local/cwaf/rules' -> /usr/local/cwaf/tmp/EMPTY'
LOG : /usr/local/cwaf/logs' -> /var/log/CWAF'
LOG : /etc/cwaf' -> /usr/local/cwaf/etc'
LOG : Preparing DirectAdmin configuration
LOG : | LOG : Preparing file /usr/local/cwaf/web/cwaf/js/cwaf.js
LOG : | LOG : Preparing file /usr/local/cwaf/web/cwaf/js/cwaf_catalog.js
LOG : | LOG : Preparing file /usr/local/cwaf/web/cwaf/js/cwaf_wizard.js
LOG : | LOG : Preparing file /usr/local/cwaf/web/cwaf/js/cwaf_wizard_ref.js
LOG : Setting Up ModSecurity config
LOG : /etc/httpd/conf/extra/httpd-modsecurity.conf' -> /usr/local/cwaf/conf/modsec2_plugin.conf'
LOG : All Done!
-----
Installation complete!
You may examine log file
/tmp/cwaf_install.log.29436
for errors in case not everything went flawless.
Also you may examine file
/usr/local/cwaf/INFO.TXT
for some useful software information.
-----
Installation of ModSecurity Rule Set has been finished.
Stopping httpd: [ OK ]
```

...and on successful completion, the CWF plugin will be available in the 'Extra Features' section.



The CWF plugin allows administrators to update and manage Comodo ModSecurity protection rules. Refer to the next section '[Using the CWF Plugin for Firewall Configuration](#)' for more details.

## 2.1. Using the CWF Plugin for Firewall Configuration

CWF plugin allows administrators to view and modify firewall configuration, update the rule sets, configure rules to be excluded from the currently loaded rule set and to submit feedback to Comodo on the currently loaded rules.

### To access the CWF DirectAdmin plugin

- Login to DirectAdmin on your server
- Go 'Admin Level' > 'Extra Features' > 'Comodo WAF'

The Comodo Web Application Firewall configuration screen will appear.

#### Web Application Firewall | Free ModSecurity Rules from Comodo

Main	Configuration	Security Engine	Userdata	Feedback	Catalog	Protection Wizard
Current rules version	1.03					Restore rules
CWAF plugin version	2.9					Rules 1.12 is available
Web Platform	Nginx					Client 2.11 is available
Nginx version	1.8.0					
Mod_security compatible	yes					
Mod_security loaded	yes					
Mod_security conf	/etc/nginx/nginx-modsecurity.conf					
Found websites	2					

The interface has seven tabs:

- **Main** - Displays the versions of the currently loaded rule set, Apache server, Mod-Security status and number of websites protected. Refer to '[Viewing CWAF Information](#)' page of CWAF online guide for more details.
- **Configuration** – Enables the administrator to view and edit CWAF configuration parameters. Please note that 'Schedule Rules Update' is not available for DirectAdmin since updates of rules is controlled by DA itself. Refer to '[Configuring CWAF Parameters](#)' page of CWAF online guide for more details
- **Security Engine** - Enables the administrator to set up rules for Mod\_security option. Refer to '[Managing Security Engine](#)' page of CWAF online guide for more details
- **Userdata** - Allows administrators to manage custom user settings such as custom user rules, Mod\_security options, and the parameters of currently loaded rule-sets. Refer to '[Configuring Userdata](#)' page of CWAF online guide for more details.
- **Feedback** – Enables the administrator to submit their feedback, like the false positives reported by the currently loaded version of the ruleset. Please note for DirectAdmin, this feature enabled with Comodo account only. Refer to '[Sending Feedback](#)' page of CWAF online guide for more details.
- **Catalog** - Allows administrators to specify rules that should be excluded from implementation. Refer to '[Managing Catalog](#)' page of CWAF online guide for more details.
- **Protection Wizard** – Allows administrators to enable/disable rules depending on the web applications installed on the server thus helping to significantly reduce server load. Refer to '[Protection Wizard](#)' page of CWAF online guide for more details.

# 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)