COMODO
Creating Trust Online®

Web Application Firewall
POWERED BY COMODO

Comodo
Web Application Firewall

Software Version 2.11

Administrator Guide

Guide Version 2.11.071315

Comodo Security Solutions
1255 Broad Street
Clifton, NJ 07013

Table of Contents

1. Comodo Free ModSecurity Rules - Introduction

Web applications are arguably the most important back-end component of any online business. They are used to power many of the features most of us take for granted on a website, including web-mail, online stores, software-as-a-service, payment gateways, forums, dynamic content, social media functionality and much more. A security breach on a web application can have potentially devastating implications for the site owner, including site downtime, loss of corporate data and even theft of confidential customer information. It is therefore of paramount importance that web applications are kept strongly protected against attack at all times. **Comodo Web Application Firewall** (CWAF) provides powerful, real-time protection for web applications and websites running on Apache, LiteSpeed, Nginx and Linux based web-servers.

The following implementation approaches are available:

- **Install the Comodo WAF Plugin on cPanel, DirectAdmin, Plesk** or **Webmin**

  The plugin interface will be used to download, implement and manage Comodo Mod Security rules. See '**Using The CWAF Agent**' and '**Using the Web Hosting Control Panel for Firewall Configuration**' for help with this.

- **Enable Comodo as a ModSecurity vendor in cPanel, DirectAdmin or Plesk**.

  Admins will use each panel's native controls to download, implement and manage Comodo Mod Security rules. For setup help with this option, users should refer to the standalone guides for **cPanel**, **DirectAdmin** or **Plesk**.

- **Install the Comodo WAF Plugin directly onto the webserver (aka 'Standalone' mode)**

  After installation, admins should use the CWAF console tool to manage updates. See the page '**Using the CWAF agent**', '**Using the Agent for Firewall Configuration**' and '**Command Line Utility**' for help with this.

CWAF is easy to set up and offers a customizable, rules-based traffic control system that delivers persistent protection against all known internet threats. Frequent updates to the firewall rules database means your web site is even protected against the latest, emerging hacking techniques that might be affecting other websites.

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, Webmin 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.

Currently CWAF is designed for and has been tested on Apache and LiteSpeed and Nginx on Linux servers.

Guide Structure

This guide is intended to take the administrator through the sign-up, configuration and use of Comodo Web Application Firewall.

- **Comodo Web Application Firewall - Introduction** - A high level description of the product
  - **System Requirements** - List of compatible server environments for CWAF
  - **Signing up for Web Application Firewall** - Guidance on signing-up for the product
  - **Logging-in to the Administration Console** - Guidance on logging-in to the web administration console
  - **The Administration Console - The Main Interface** - Description of the web administration console
- **Deploying CWAF rules on Server** - Guidance on downloading and deploying the firewall rule sets on to the server
  - **Using the CWAF Agent** - Guidance on using the CWAF agent for downloading and deploying the firewall rule sets
    - **Installing the Web Hosting Control Panel Plugin**
    - **Installing the Agent for Deploying the Rule Sets**
    - **Using the Web Hosting Control Panel Plugin for Firewall Configuration**
    - **Using the Agent for Firewall Configuration**
  - **Uninstalling the CWAF Agent**
  - **Downloading and installing rule set packages -** Guidance on manually downloading and deploying the firewall rule sets

- **Reporting Problems to Comodo** - Guidance on posting feedback to Comodo
- **Submitting Ticket for troubleshooting –** Guidance on submitting support tickets to Comodo
- **Managing CWAF License** - Guidance on viewing and managing licenses and subscribing for other Comodo products and services

1.1. System Requirements

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

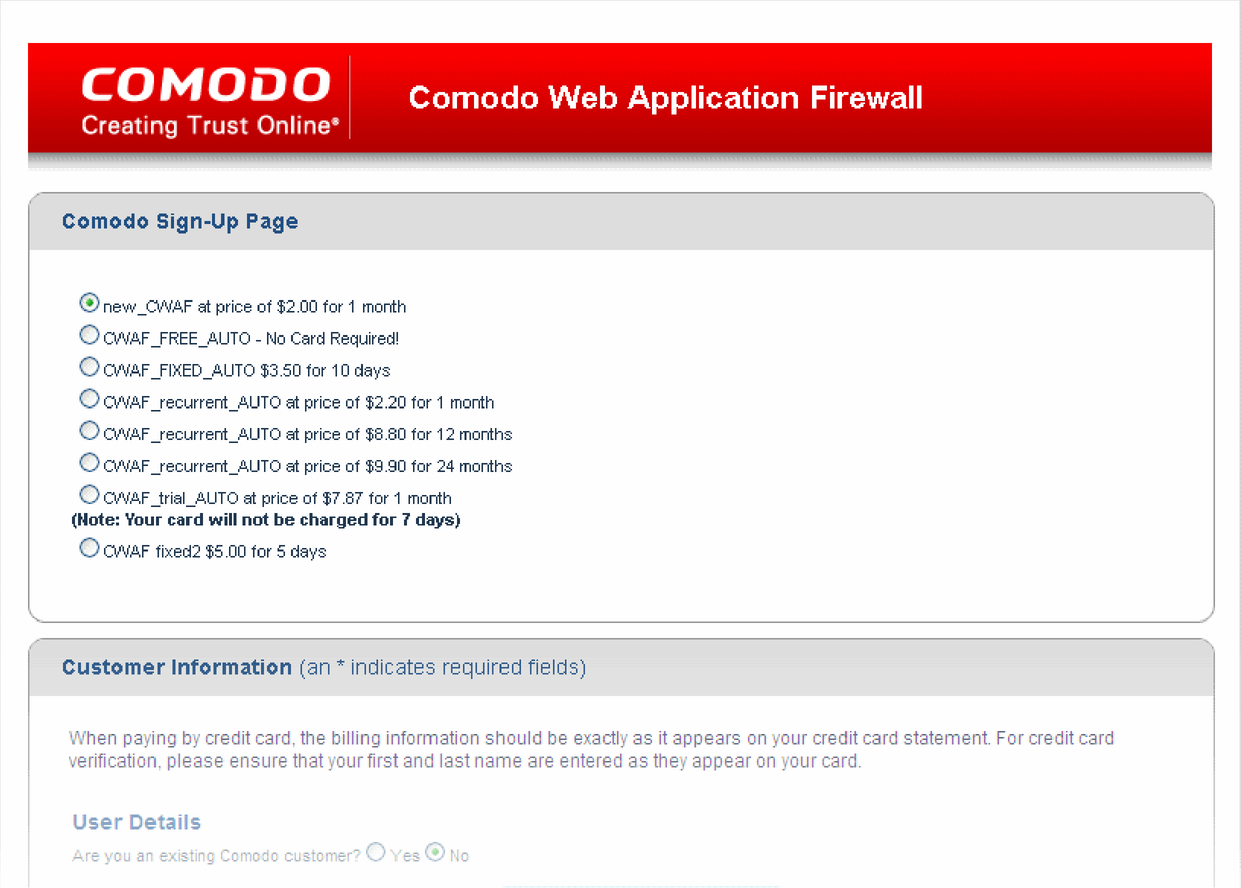
- Apache, LiteSpeed or Nginx web server on Linux server platform
- ModSecurity 2.7.5 and higher

1.2. Signing up for Free ModSecurity Rules

The administrator can sign-up for the CWAF service from the Comodo Accounts Manager at **https://accounts.comodo.com/cwaf/management/signup**.

To sign-up for CWAF

- Visit the CWAF sign-up page at **https://accounts.comodo.com/cwaf/management/signup**. The Sign-up form will appear.
- Select the CWAF product from the list



COMODO Creating Trust Online® Comodo Web Application Firewall

Comodo Sign-Up Page

● new_CWAF at price of $2.00 for 1 month
○ CWAF_FREE_AUTO - No Card Required!
○ CWAF_FIXED_AUTO $3.50 for 10 days
○ CWAF_recurrent_AUTO at price of $2.20 for 1 month
○ CWAF_recurrent_AUTO at price of $8.80 for 12 months
○ CWAF_recurrent_AUTO at price of $9.90 for 24 months
○ CWAF_trial_AUTO at price of $7.87 for 1 month
(Note: Your card will not be charged for 7 days)
○ CWAF fixed2 $5.00 for 5 days

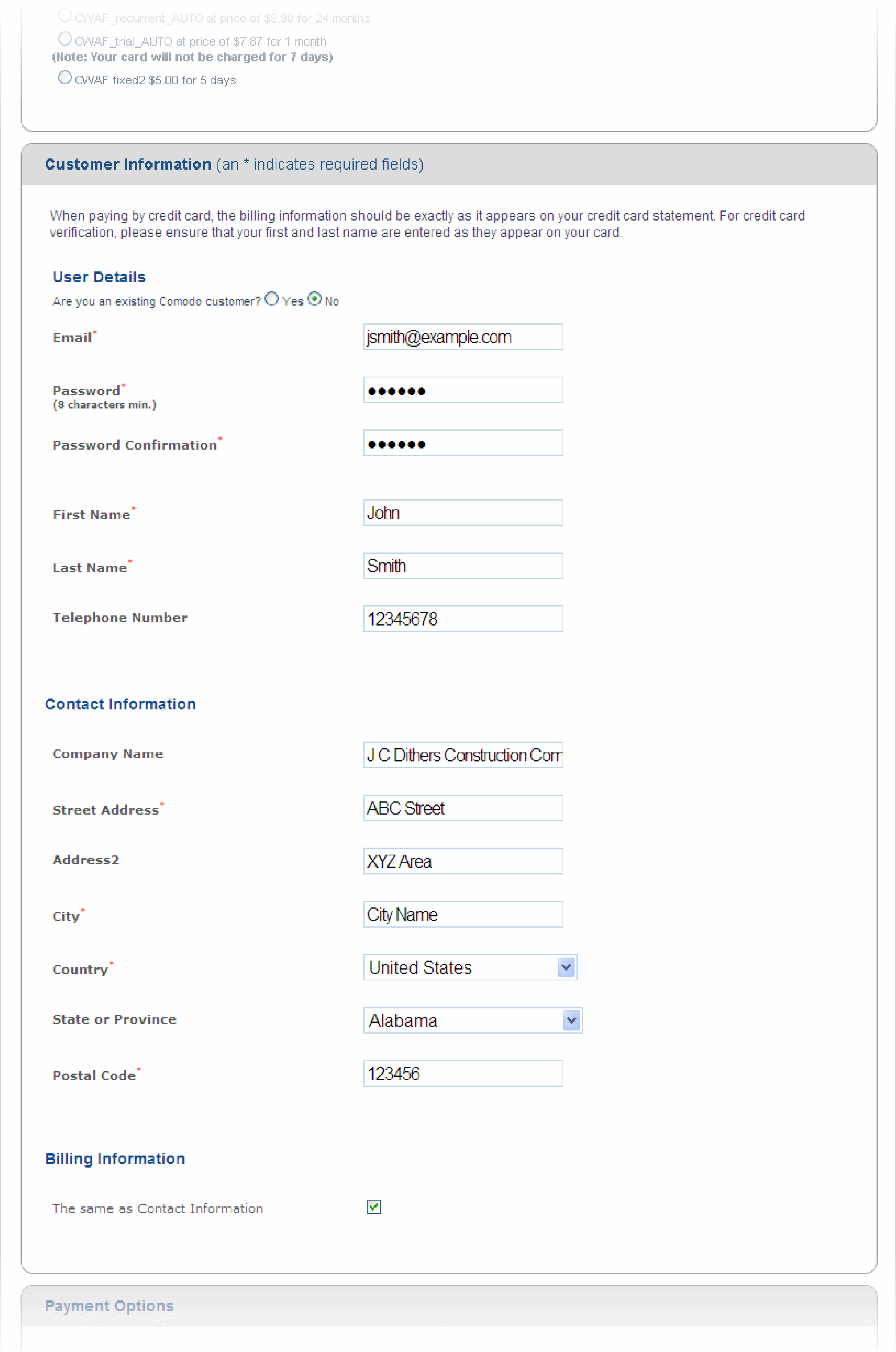
Customer Information (an * indicates required fields)

When paying by credit card, the billing information should be exactly as it appears on your credit card statement. For credit card verification, please ensure that your first and last name are entered as they appear on your card.

User Details

Are you an existing Comodo customer? ○ Yes ● No

- Select the CWAF product from the list



○ CWAF_recurrent_AUTO at price of $9.90 for 24 months
○ CWAF_trial_AUTO at price of $7.87 for 1 month
(Note: Your card will not be charged for 7 days)
○ CWAF fixed2 $5.00 for 5 days

Customer Information (an * indicates required fields)

When paying by credit card, the billing information should be exactly as it appears on your credit card statement. For credit card verification, please ensure that your first and last name are entered as they appear on your card.

User Details

Are you an existing Comodo customer? ○ Yes ● No

Email*	jsmith@example.com
Password* (8 characters min.)	●●●●●●
Password Confirmation*	●●●●●●
First Name*	John
Last Name*	Smith
Telephone Number	12345678

Contact Information

Company Name	J C Dithers Construction Com
Street Address*	ABC Street
Address2	XYZ Area
City*	City Name
Country*	United States
State or Province	Alabama
Postal Code*	123456

Billing Information

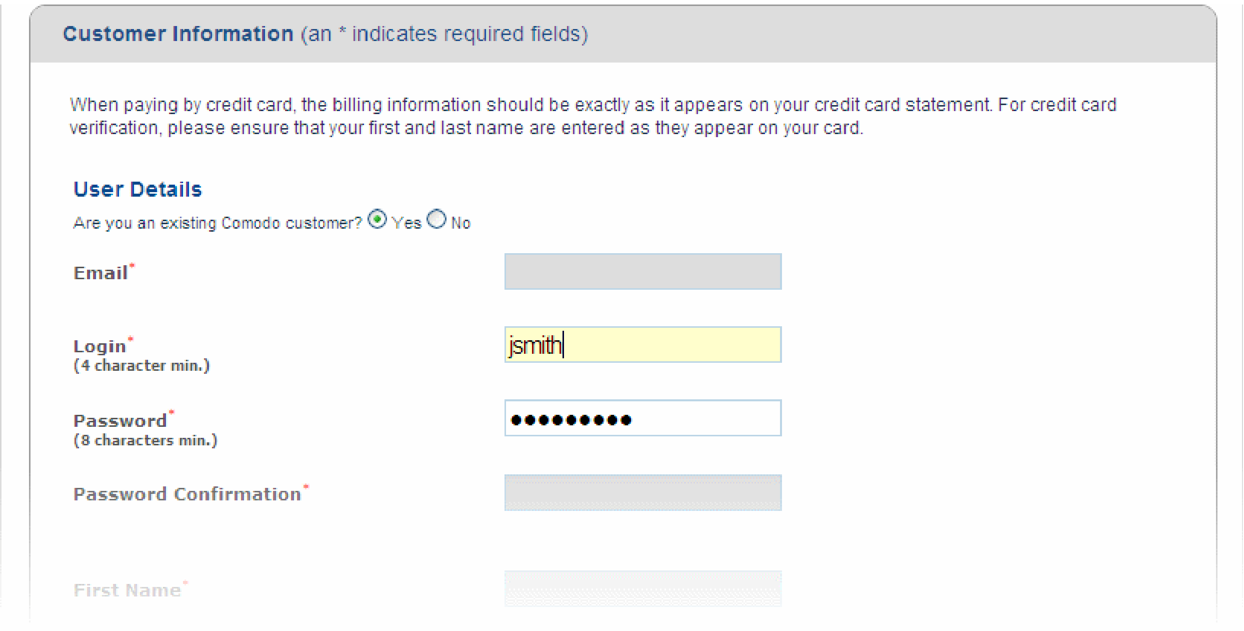
The same as Contact Information ☑

Payment Options

User Details:

- If you are a new to customer, select 'No' for 'Are you an existing Comodo customer?' and enter the details
- If you already have an account at Comodo Accounts Manager created while subscribing for some other product or you

are renewing the CWAF license, select 'Yes' for 'Are you an existing Comodo customer?'. You will need to fill only your username and password.



Customer Information (an * indicates required fields)

When paying by credit card, the billing information should be exactly as it appears on your credit card statement. For credit card verification, please ensure that your first and last name are entered as they appear on your card.

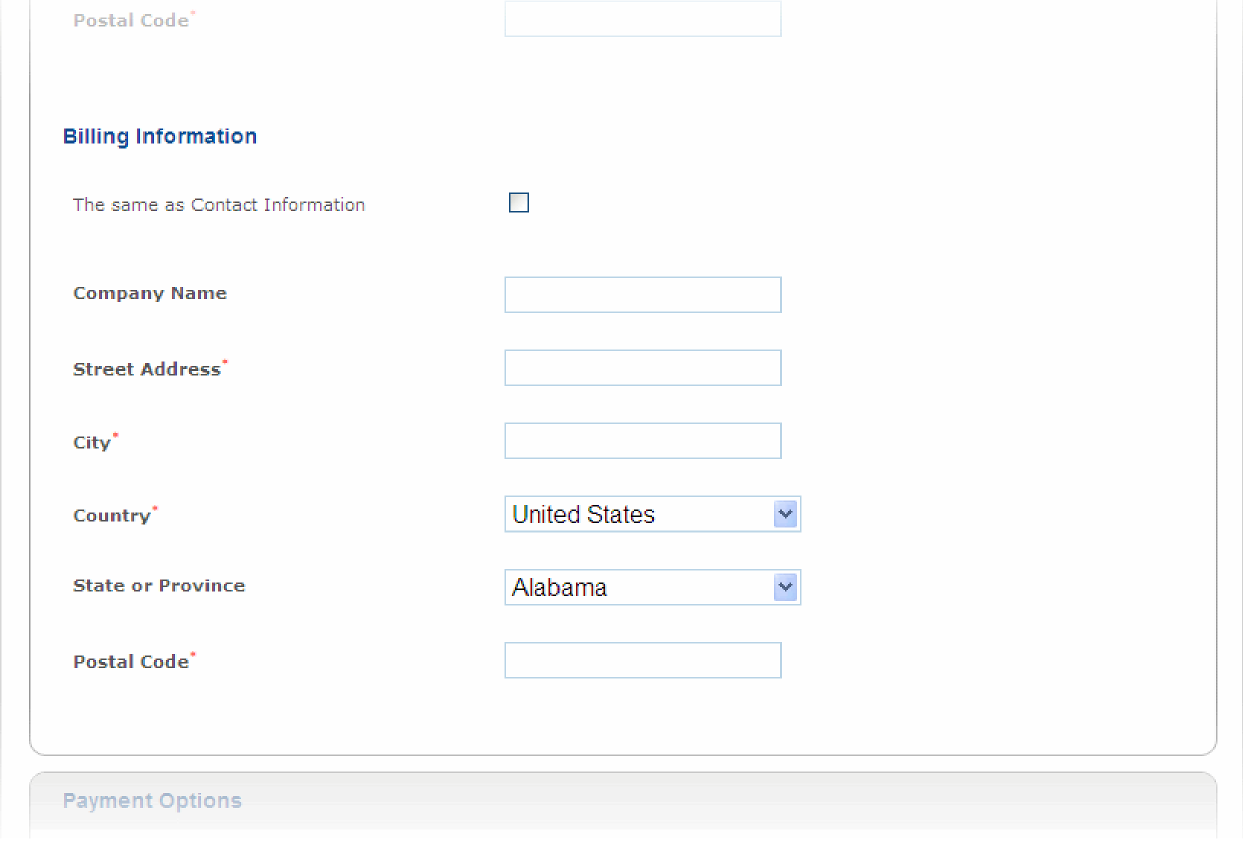
User Details

Are you an existing Comodo customer? ● Yes ○ No

Email*	
Login* (4 character min.)	jsmith
Password* (8 characters min.)	•••••••••
Password Confirmation*	
First Name*	

Contact Information and Billing Information:

- Enter the details in the appropriate fields. The fields marked with * are mandatory.
- If the Billing address is different from the contact information, deselect the 'The same as Contact Information' check box and enter the billing address.



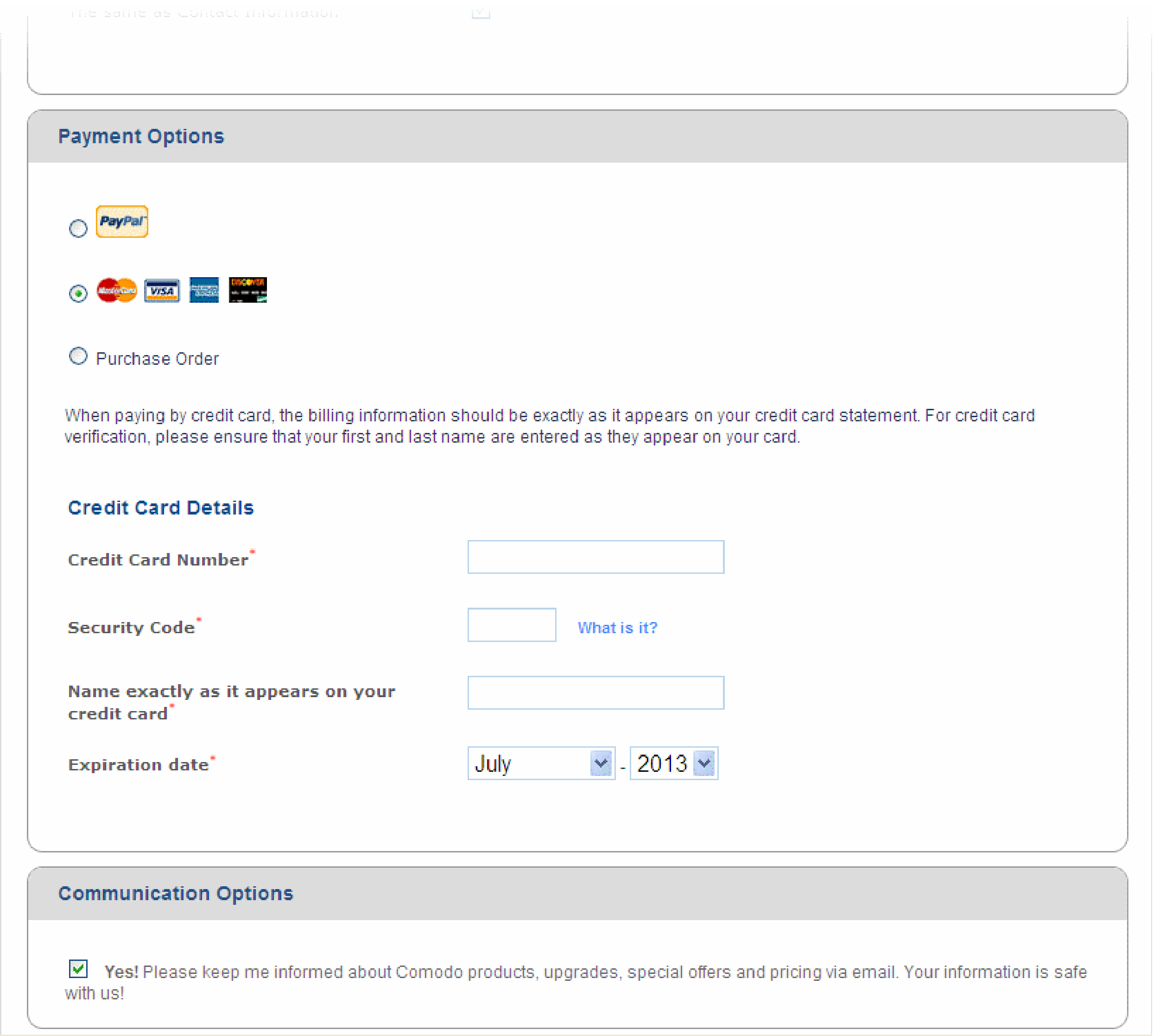
Postal Code*	

Billing Information

The same as Contact Information	□
Company Name	
Street Address*	
City*	
Country*	United States
State or Province	Alabama
Postal Code*	

Payment Options

Payment Options:



The same as Contact Information

Payment Options

○ PayPal

●

○ Purchase Order

When paying by credit card, the billing information should be exactly as it appears on your credit card statement. For credit card verification, please ensure that your first and last name are entered as they appear on your card.

Credit Card Details

Credit Card Number*	
Security Code*	What is it?
Name exactly as it appears on your credit card*	
Expiration date*	July - 2013

Communication Options

☑ **Yes!** Please keep me informed about Comodo products, upgrades, special offers and pricing via email. Your information is safe with us!

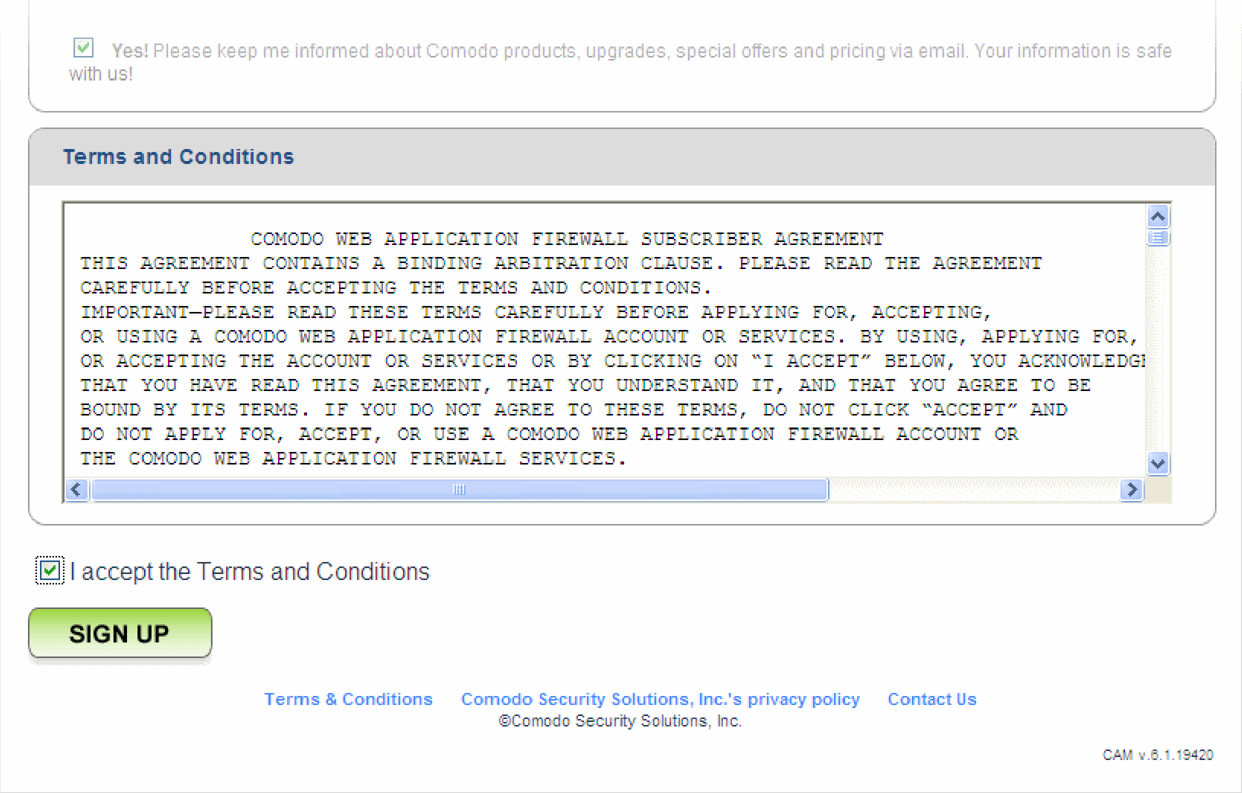
- Select your payment mode in the 'Payment Options' section and enter the required details in the respective fields.

Communication Options:

- If you wish to sign up for news about Comodo products, select the check box under the 'Communication Options'. The periodical news and announcements from Comodo on new product releases, special offers upgrades and so on, will be notified to you through email.

Terms and Conditions:

- Read the 'End User License and Subscriber Agreement' and accept to it by selecting 'I accept the Terms and Conditions' checkbox.



☑ Yes! Please keep me informed about Comodo products, upgrades, special offers and pricing via email. Your information is safe with us!

Terms and Conditions

```
                COMODO WEB APPLICATION FIREWALL SUBSCRIBER AGREEMENT
THIS AGREEMENT CONTAINS A BINDING ARBITRATION CLAUSE. PLEASE READ THE AGREEMENT
CAREFULLY BEFORE ACCEPTING THE TERMS AND CONDITIONS.
IMPORTANT—PLEASE READ THESE TERMS CAREFULLY BEFORE APPLYING FOR, ACCEPTING,
OR USING A COMODO WEB APPLICATION FIREWALL ACCOUNT OR SERVICES. BY USING, APPLYING FOR,
OR ACCEPTING THE ACCOUNT OR SERVICES OR BY CLICKING ON "I ACCEPT" BELOW, YOU ACKNOWLEDGI
THAT YOU HAVE READ THIS AGREEMENT, THAT YOU UNDERSTAND IT, AND THAT YOU AGREE TO BE
BOUND BY ITS TERMS. IF YOU DO NOT AGREE TO THESE TERMS, DO NOT CLICK "ACCEPT" AND
DO NOT APPLY FOR, ACCEPT, OR USE A COMODO WEB APPLICATION FIREWALL ACCOUNT OR
THE COMODO WEB APPLICATION FIREWALL SERVICES.
```

☑ I accept the Terms and Conditions

SIGN UP
Terms & Conditions
Comodo Security Solutions, Inc.'s privacy policy
Contact Us
©Comodo Security Solutions, Inc.
CAM v.6.1.19420

- Click 'SIGN UP'

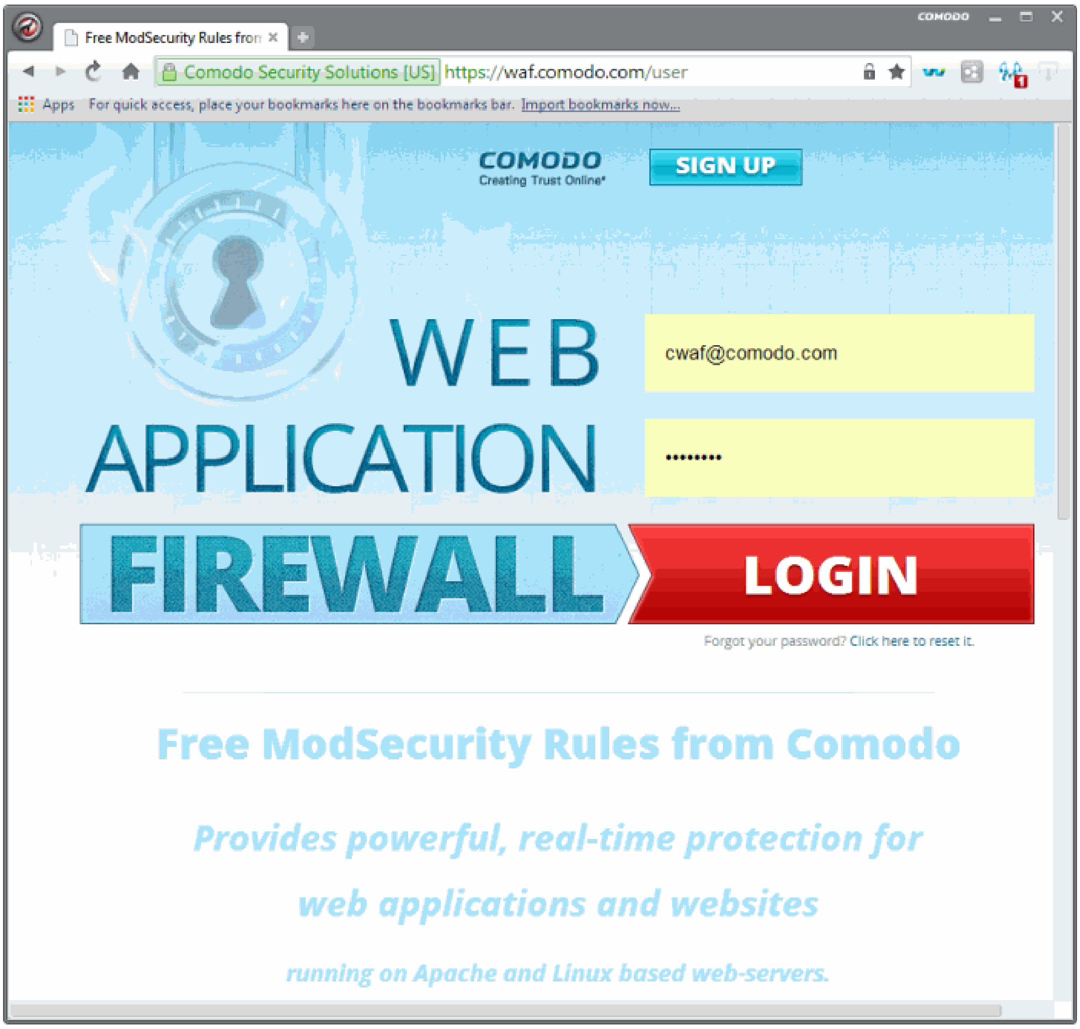
Upon successful payment processing, your account will be activated. You can sign-in to the Comodo Web Application Firewall administration interface at **https://waf.comodo.com** with the same username and password you created or used during enrollment.

Further Reading:

- **Logging-in to the Administration Console**
- **Deploying CWAF rules on Server**

1.3. Logging-in to the Administration Console

The Administrator can log-in to the Comodo Web Application Firewall administration interface at **https://waf.comodo.com**.

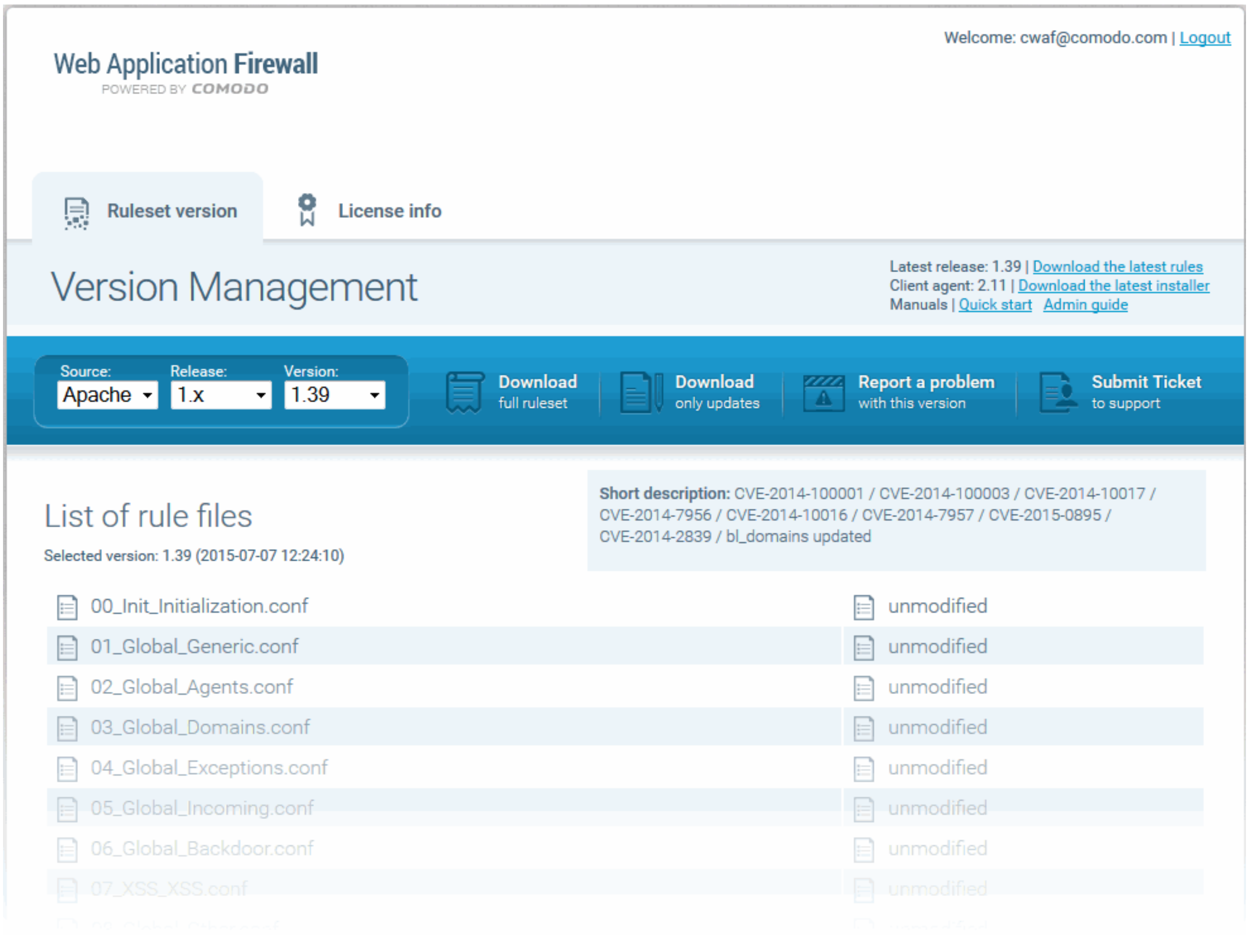

Free ModSecurity Rules fron
Comodo Security Solutions [US] https://waf.comodo.com/user
Apps For quick access, place your bookmarks here on the bookmarks bar. Import bookmarks now...
COMODO Creating Trust Online
SIGN UP
WEB APPLICATION FIREWALL
LOGIN
Forgot your password? Click here to reset it.
Free ModSecurity Rules from Comodo
Provides powerful, real-time protection for web applications and websites
running on Apache and Linux based web-servers.

cwaf@comodo.com

••••••••

- Enter your login username and password specified during signing-up
- Click 'Login'

You will be taken to the CWAF web administration console.



Welcome: cwaf@comodo.com | Logout

Web Application Firewall
POWERED BY COMODO

Version Management

Latest release: 1.39 | Download the latest rules
Client agent: 2.11 | Download the latest installer
Manuals | Quick start Admin guide

Source: Apache
Release: 1.x
Version: 1.39

List of rule files

Selected version: 1.39 (2015-07-07 12:24:10)

Short description: CVE-2014-100001 / CVE-2014-100003 / CVE-2014-10017 / CVE-2014-7956 / CVE-2014-10016 / CVE-2014-7957 / CVE-2015-0895 / CVE-2014-2839 / bl_domains updated

00_Init_Initialization.conf	unmodified
01_Global_Generic.conf	unmodified
02_Global_Agents.conf	unmodified
03_Global_Domains.conf	unmodified
04_Global_Exceptions.conf	unmodified
05_Global_Incoming.conf	unmodified
06_Global_Backdoor.conf	unmodified
07_XSS_XSS.conf	unmodified

1.4. The Administration Console - The Main Interface

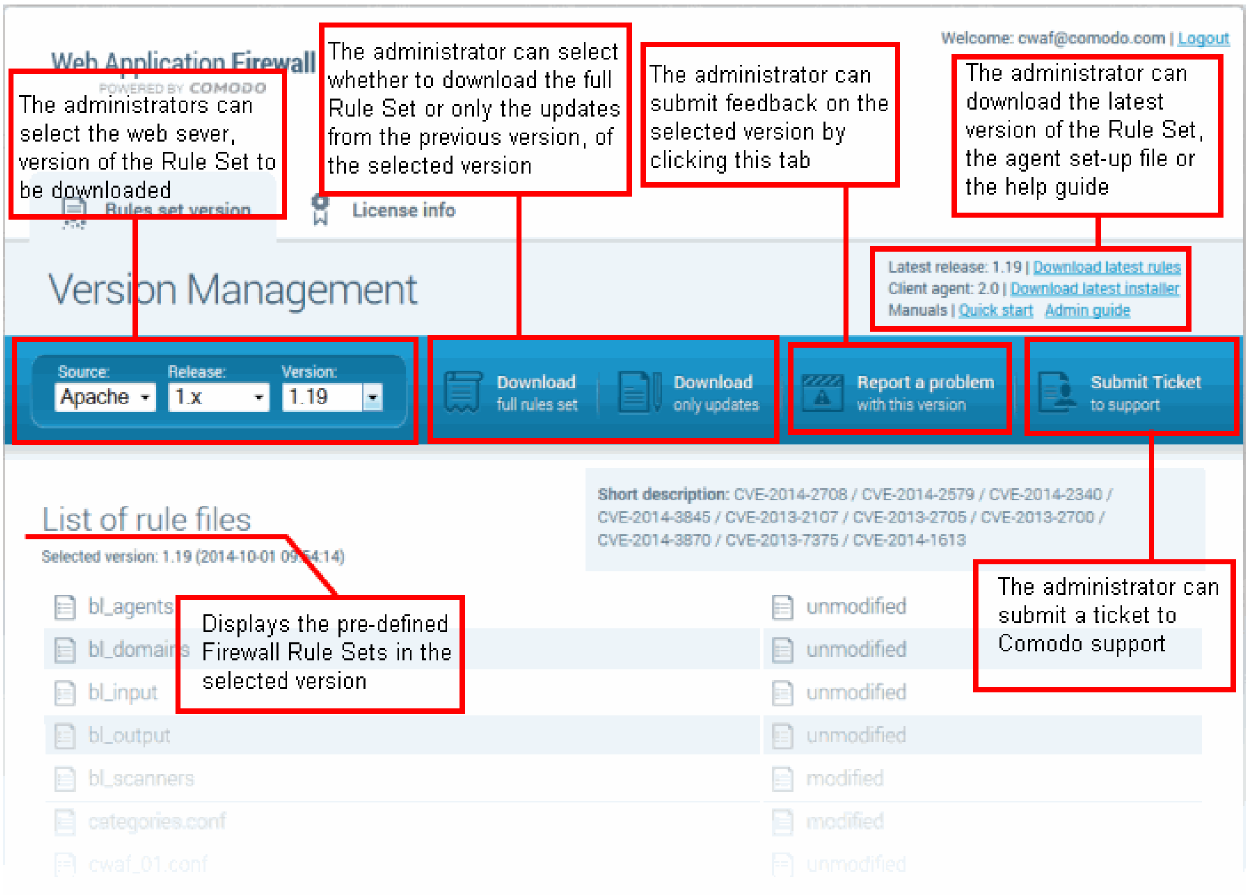
Comodo Web Application Firewall controls inbound and outbound traffic to/from a protected web application based on the firewall ruleset that has been specified for that application. The admin console enables the administrator to download pre-defined rule-sets and to deploy them on their web application servers. The administrator can also download and install an agent that will automatically download and implement the rule-sets and which will update them whenever the rules are updated by Comodo. The agent also installs a Web Hosting Control Panel plugin (cPanel, Plesk, DirectAdmin and Webmin) that facilitates the configuration of updates and management of mod_security. The Administrator can also view, renew or upgrade the CWAF license from the administration interface.

The administration interface contains two tabs:

- **Rules Set Version**
- **License Info**

Rule Set Version

The Rule Set Version tab displays the rulesets that can be downloaded. The Administrator can select the version of ruleset to be downloaded or can download the CWAF agent from this interface.


Web Application Firewall
POWERED BY COMODO
Welcome: cwaf@comodo.com | Logout
Rules set version
License info
Version Management
Latest release: 1.19 | Download latest rules
Client agent: 2.0 | Download latest installer
Manuals | Quick start Admin guide
Source: Apache
Release: 1.x
Version: 1.19
Download full rules set
Download only updates
Report a problem with this version
Submit Ticket to support
List of rule files
Selected version: 1.19 (2014-10-01 09:54:14)
Short description: CVE-2014-2708 / CVE-2014-2579 / CVE-2014-2340 / CVE-2014-3845 / CVE-2013-2107 / CVE-2013-2705 / CVE-2013-2700 / CVE-2014-3870 / CVE-2013-7375 / CVE-2014-1613
bl_agents
bl_domains
bl_input
bl_output
bl_scanners
categories.conf
cwaf_01.conf
unmodified
unmodified
unmodified
unmodified
modified
modified
unmodified

The administrators can select the web sever, version of the Rule Set to be downloaded

The administrator can select whether to download the full Rule Set or only the updates from the previous version, of the selected version

The administrator can submit feedback on the selected version by clicking this tab

The administrator can download the latest version of the Rule Set, the agent set-up file or the help guide

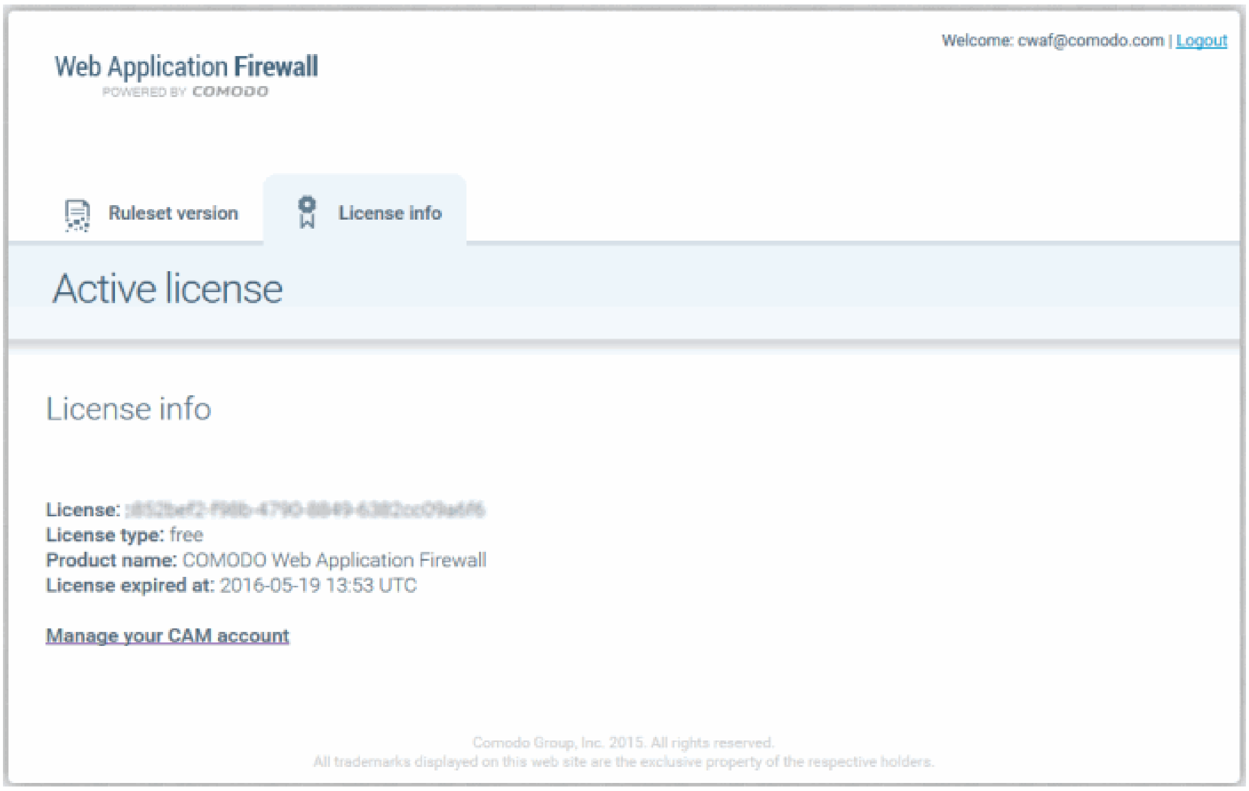
Displays the pre-defined Firewall Rule Sets in the selected version

The administrator can submit a ticket to Comodo support

- **Source Version Management** - The administrator can choose the source version of the Firewall Rule Set to be downloaded from the drop-down options under 'Version Management'
- **Rule Set Selection** - The administrator can choose to download the full rule set or only the updates in the selected rule set with respect to the previous version, by clicking the respective tabs
- **Ruleset/Agent Download** - The administrator can choose to directly download the latest ruleset or the CWAF agent for installation on to the server by clicking the respective links at the top right.
- **Report a Problem** - The administrator can submit feedback, like false positives reported by the selected version of the rule set by clicking the Report a Problem tab
- **Submit a Ticket** – Administrators can submit support tickets at **https://support.comodo.com/**
- **List of rule files** - Displays the firewall rules included in the currently selected rule set version

License Info

The 'License Info' tab displays the account license key, license type and license expiry date. The interface also has a link to Comodo Accounts Manager to enable the administrator to renew or upgrade the license.



Welcome: cwaf@comodo.com | Logout

Active license

License info

License: [redacted]
License type: free
Product name: COMODO Web Application Firewall
License expired at: 2016-05-19 13:53 UTC

Manage your CAM account

Comodo Group, Inc. 2015. All rights reserved.
All trademarks displayed on this web site are the exclusive property of the respective holders.

2. Deploying CWAF Rules On Server

Comodo Web Application Firewall allows or denies access to the web application by the requests from external and the data forwarded to external by the web application depending on the Firewall Rule sets specified for the application. Firewall Rule sets are, in turn, made up from one or more individual firewall rules. Each individual firewall rule contains instructions that determine whether the application should be allowed or blocked; which protocols it is allowed to use; which ports it is allowed to use and so forth.

Comodo periodically publishes pre-defined firewall rule sets for the CWAF, which can be downloaded by the administrators from the CWAF web administration console. The administrator can deploy these rule sets on to their web application server. The administrator can periodically receive the updated versions of the rule sets from the web interface for deployment.

One more way for the administrators to deploy the up-to-date firewall rule sets is by the use of CWAF Agent. As a one-off process, the administrator can download the agent set-up from the web administration interface and install it on the web application server. The agent can be configured to:

- Periodically poll the CWAF server and to automatically download and install the up-to-date firewall rule sets
- Install a Web Hosting Control Panel plugin on to the server that facilitates the administrator to configure the CWAF implementation

Refer to the following sections for more details on deploying the rulesets:

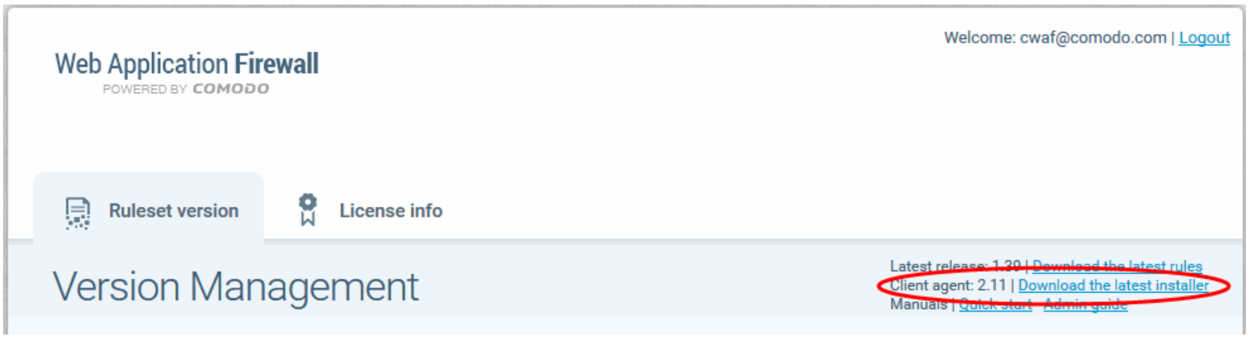
- **Using the CWAF Agent**
- **Downloading and installing rule set package**

2.1. Using the CWAF Agent

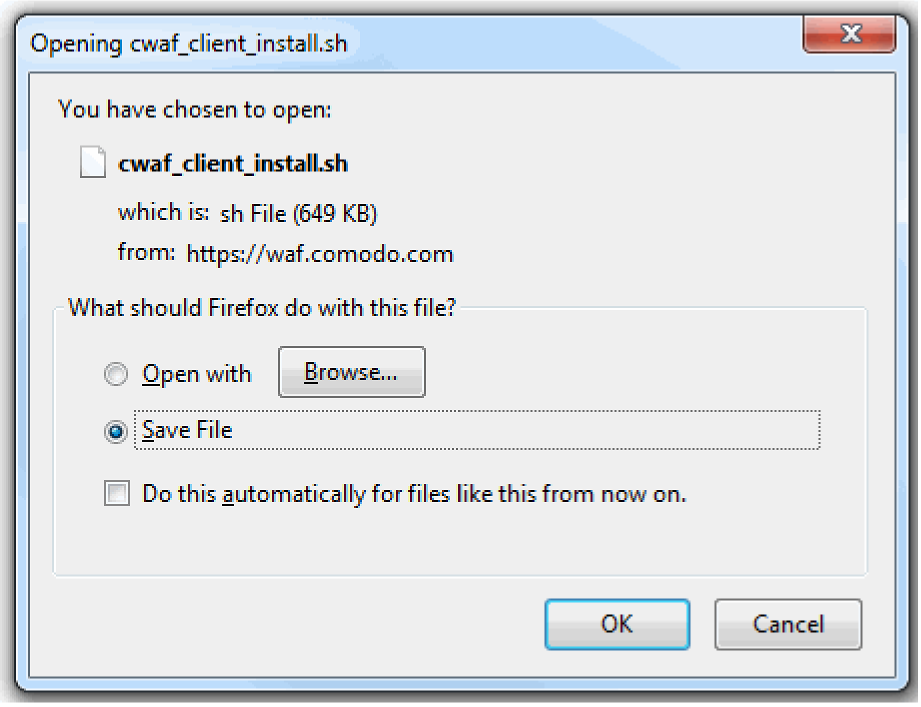
The Comodo Web Application Firewall (CWAF) agent is a small piece of software that can be installed on to the web server to automate the deployment of the periodically published pre-defined set of firewall rule sets on to the web server and to configure the CWAF.

To download the CWAF agent installation file

- Log-in to the web administration console at **https://waf.comodo.com**
- Ensure that the 'Rule set version' tab is opened
- Click the 'Download latest installer' link at the top right


Web Application Firewall
POWERED BY COMODO
Welcome: cwaf@comodo.com | Logout
Ruleset version
License info
Version Management
Latest release: 1.30 | Download the latest rules
Client agent: 2.11 | Download the latest installer
Manuals | Quick start   Admin guide

The download dialog will appear.


Opening cwaf_client_install.sh

You have chosen to open:

cwaf_client_install.sh

which is: sh File (649 KB)

from: https://waf.comodo.com

What should Firefox do with this file?

○ Open with

● Save File

□ Do this automatically for files like this from now on.

- Select 'Save' to save the file in a local drive.

The CWAF Agent checks operating system for available web hosting control panel and web server software (Apache, LiteSpeed, Nginx) and then installs the corresponding web hosting control panel plugin (cPanel plugin, Plesk plugin, DirectAdmin plugin and Webmin plugin or standalone scripts).

Refer to the sections below for more details.

- **Installing the Web Hosting Control Panel plugin** – Installing the plug-in will allow you to configure CWAF via your web host control panel.
- **Installing the agent for deploying Rule Sets** - The agent will be installed in the server will not contain any web hosting control panel. The agent will periodically check the CWAF server for updates in the rule sets and automatically download and install latest rule sets on to the server.

2.1.1. Installing the Web Hosting Control Panel Plugin

To install the web hosting control panel on to the server

- Transfer the agent setup file to a local folder in the server

  E.g. `/root`

- Run it installation script with a root privileges:

  # bash /root/cwaf_client_install.sh

Step 1

After the script is running, the CWAF Agent will check to identify the web-server type and version:

1) Check for Apache and its version:

If Apache is not running, the following warning message will be displayed: *Running Apache required to check* **ModSecurity** *version* ".

If mod_security for Apache is not found, the following warning message will be displayed: *"No installed ModSecurity for Apache found".*

If an unsupported version of mod_security for Apache is detected, the following warning message will be displayed: *"Warning: installed mod_security version is NOT fully tested" .*

2) Check for LiteSpeed and LiteSpeed mod_security:

If LiteSpeed is not found, the following warning message will be displayed: *"Not found LiteSpeed web server with mod_security enabled"*

3) Check for Nginx:

If Nginx is not found, the following warning message will be displayed: *Not found Nginx web server with mod_security enabled*

4) Checking for prerequisites:

If no web servers are found, the following warning message will be displayed: "Not found suitable web server, exiting".

If mod_security is not detected, the following warning message will be displayed: "Not found mod_security, exiting".

5) Check for web hosting control panel (cPanel, DirectAdmin, Webmin, Plesk, standalone etc)

If no web hosting management panel is found, you will be asked if you wish to "Continue in 'standalone' mode?"

If a web hosting control panel is found, the installer will ask for further action (or will display info in Update mode).

For example, if Plesk is detected it will say: "Found Plesk version PLESK_VERSION, continue installation?

Ensure SUDO utility is installed for the web hosting management panel (Plesk). Otherwise the following warning message will be displayed: *"Not found /etc/sudoers.d directory. SUDO required for Plesk plugin*

6) Check for required Perl modules:

CWAF will check for Perl modules and install them if required

If Perl modules are missing in Update mode, the following error message will be displayed: *"Some required perl modules are missed, exiting"*

If a module is missing during installation, the following warning message will be displayed: *"Some required perl modules are missed. Install them? This can take a while"*

- Click 'No' to decline Perl modules auto-installation. The following message will be displayed:"Please install perl modules [PERL MISSED MODULES] manually and run installation script again"
- If problems were detected, the warning message will be displayed: "CPAN is not configured! Please run [CPAN BIN] and configure it manually, then rerun this installation"
- After successful installation, the following message will be displayed: "DONE, PRESS ENTER":

Step 2

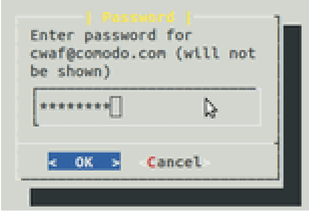
Select the web platform:

- If multiple web servers are found, select the one you prefer. The following message will be displayed: "Please select your WEB platform". Otherwise, the following warning will be displayed: "WEB platform is not selected"

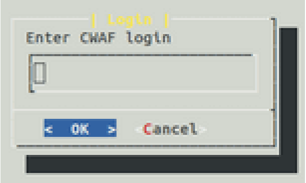
- If the selected web platform isn't supported, the following warning message will be displayed "Selected WEB platform [PLATFORM] is not supported" and installation will be terminated.

Step 3

- Enter login credentials for Comodo Web Application Firewall



```
| Password |
Enter password for
cwaf@comodo.com (will not
be shown)
********
```



```
| Login |
Enter CWAF login
```

The agent will be installed on the server at */var/cpanel/cwaf* with a cPanel plugin or at */usr/local/cwaf* with a Plesk plug-in. For more details on configuring CWAF and using the plug-in, refer to the section **Using Web Hosting Control Panel plugin for Firewall Configuration.**

2.1.2. Installing the Agent for Deploying the Rule Sets

To install the agent on to the server

- Transfer the agent setup file to a local folder in the server

  E.g. `/root`

- Run it installation script with a root privileges:

  # bash /root/cwaf_client_install.sh

If no web hosting management panel is found, the Agent will be installed in standalone mode. The Installation steps for the standalone mode are the same as for the plug-in. Refer to **Installing the Web Hosting Control Panel Plugin** for more details.

Step 4

Required for installation in standalone mode

Modify Apache Web Server configuration to enable 'mod_security' module and include CWAF Rules, by adding the key '*Include <CWAF_INSTALL_PATH>/etc/cwaf.conf*' to *'mod_security' configuration file.*

For instance, add this string to Apache HTTPD Mod_security config in your system:

Include "/opt/cwaf/etc/cwaf.conf"

and reload Apache

After Installation is complete, please restart Apache server.

The agent, in this example, is installed on the server at the path */opt/cwaf*. For more details on configuring CWAF using the agent, refer to the section **Using the Agent for Firewall Configuration**.

2.1.3. Using the Web Hosting Control Panel Plugin for Firewall Configuration

CWAF Web Hosting Control Panel 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 CWAF cPanel plugin

- Login to cPanel on your server
- Click 'Plugins' > "Comodo WAF".

To access the CWAF DirectAdmin plugin

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

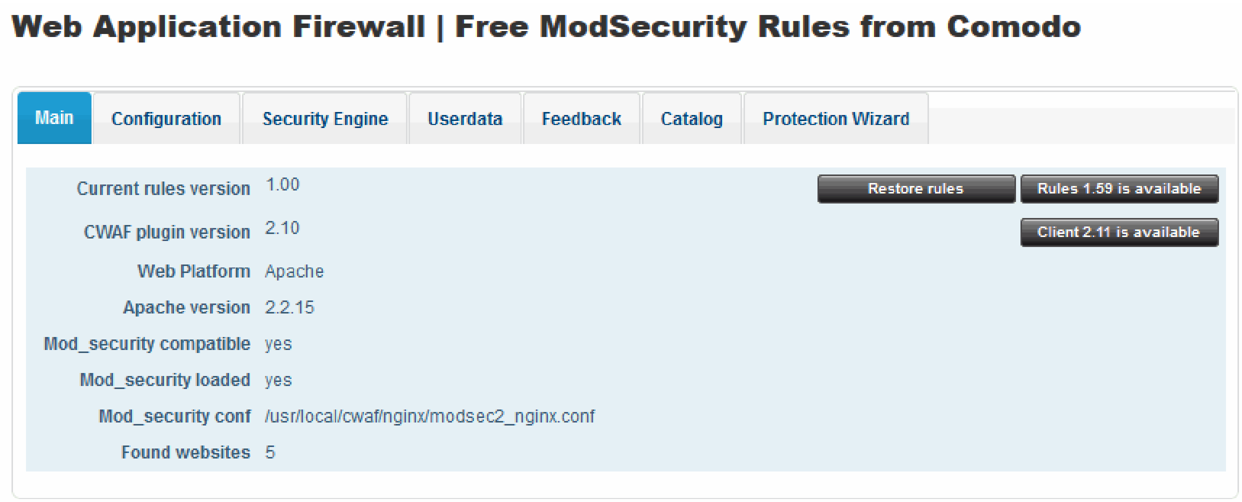
To access the CWAF Plesk plugin

- Login to Plesk on your server
- Click 'Extensions' > "Comodo WAF Plugin".

To access the CWAF Webmin plugin

- Login to Webmin on your server
- Click on 'Servers' > 'Comodo WAF'

The Comodo Web Application Firewall configuration screen will appear.



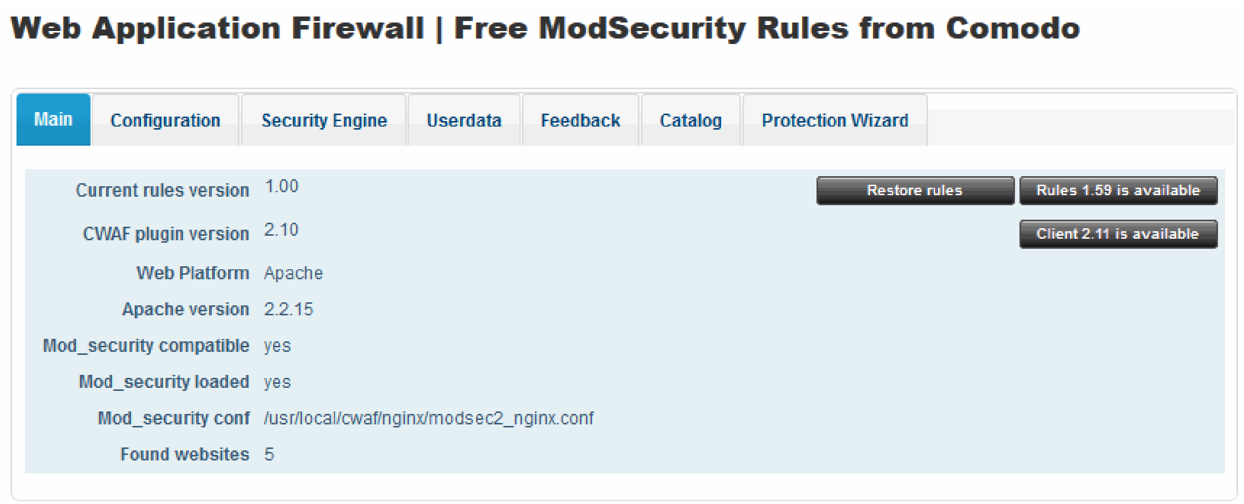
Current rules version	1.00
CWAF plugin version	2.10
Web Platform	Apache
Apache version	2.2.15
Mod_security compatible	yes
Mod_security loaded	yes
Mod_security conf	/usr/local/cwaf/nginx/modsec2_nginx.conf
Found websites	5

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**' for more details
- **Configuration** – Enables the administrator to view and edit CWAF configuration parameters. Refer to '**Configuring CWAF Parameters**' for more details
- **Security Engine** - Enables the administrator to set up rules for Mod_security option. Refer to **Managing Security Engine** 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** for more details.
- **Feedback** – Enables the administrator to submit their feedback, like the false positives reported by the currently loaded version of the ruleset. Refer to '**Sending Feedback**' for more details.
- **Catalog** - Allows administrators to specify rules that should be excluded from implementation. Refer to **Managing Catalog** 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'** for more details.

2.1.3.1. Viewing and Updating CWAF Information

The 'Main' tab of the CWAF Web Hosting Control Panel plugin configuration screen displays version information about CWAF components and your web server software. The Main tab enables administrators to download the latest CWAF plugin, to manually update the currently loaded rule set to the latest version or to restore to previous rules version.



Web Application Firewall | Free ModSecurity Rules from Comodo

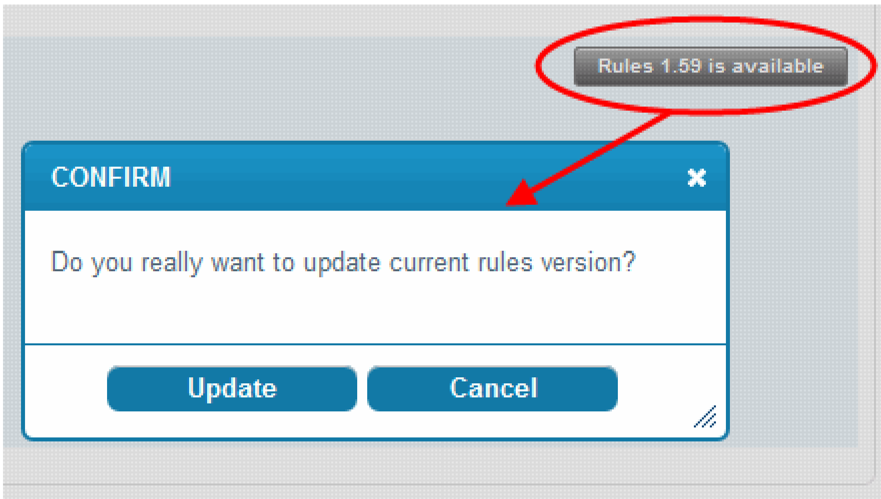
Current rules version	1.00
CWAF plugin version	2.10
Web Platform	Apache
Apache version	2.2.15
Mod_security compatible	yes
Mod_security loaded	yes
Mod_security conf	/usr/local/cwaf/nginx/modsec2_nginx.conf
Found websites	5

- **Current rules version** - Displays the version number of the currently loaded rules set
- **CWAF plugin version** – Displays the currently installed CWAF plugin version
- **Web Platform** - Displays the used source of web server
- **Apache version** - Displays the version number of web server
- **Mod_security compatible** - Indicates whether the current Apache configuration is compatible with the web application layer firewall 'Mod_Security'
- **Mod_security loaded** - Indicates whether the web application layer firewall 'Mod_Security' is currently loaded on the Apache
- **Mod_security conf** - Indicates the location of Mod_Security configuration files
- **Found websites** - Indicates number of websites hosted by Apache.

To download the latest rule sets version

- Login to cPanel on your server
- Click 'Plugins' > "Comodo WAF".
- Click the 'Rules X.XX is available' at the far right side of the interface

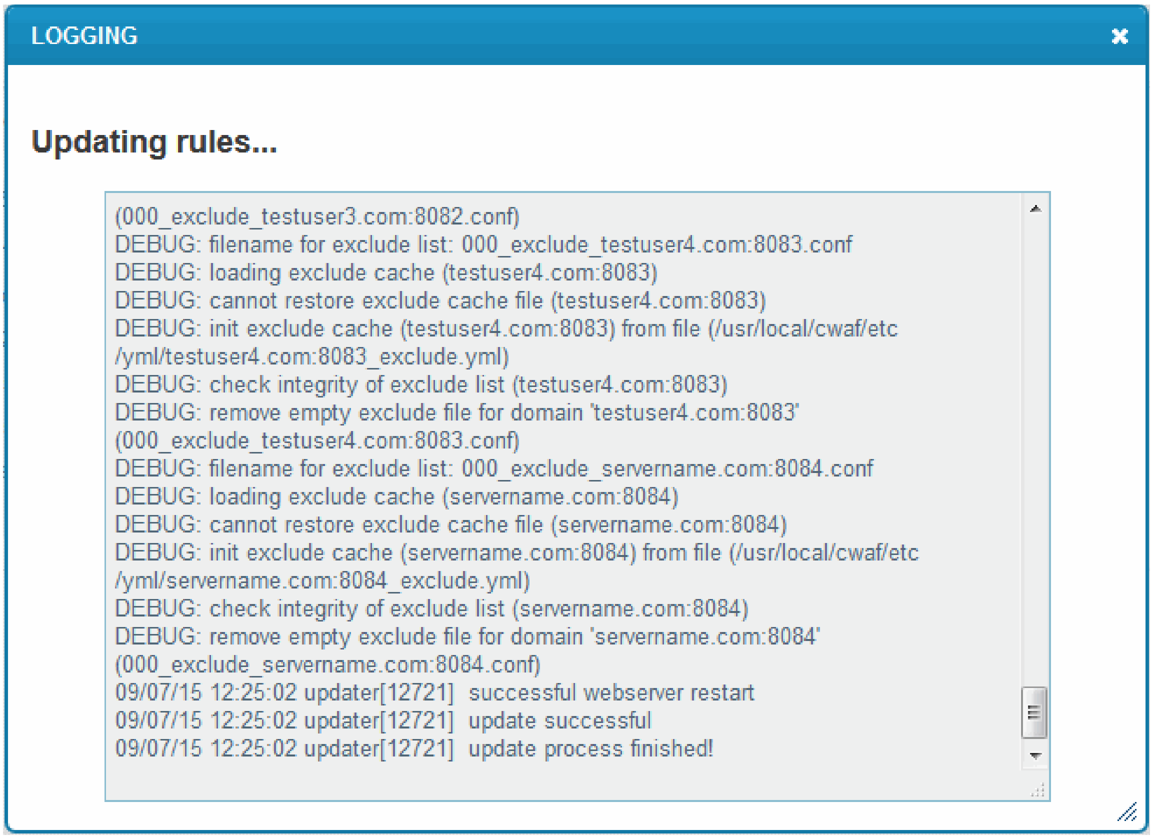
The confirmation message will be displayed.



Do you really want to update current rules version?

Click 'Update'.

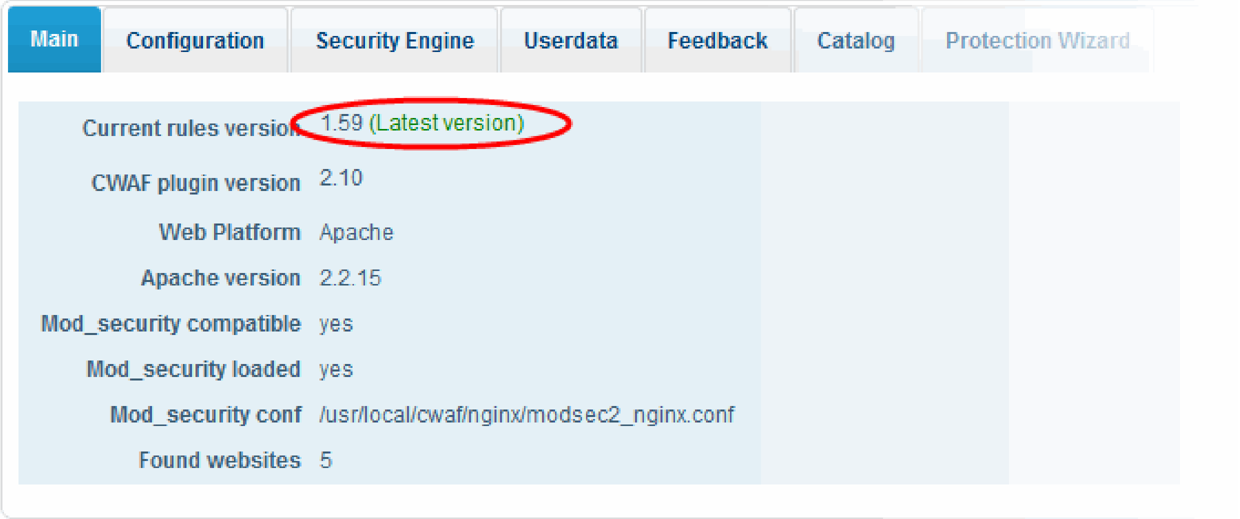
The updater will automatically download and deploy the latest version of rule set.



Updating rules...

```
(000_exclude_testuser3.com:8082.conf)
DEBUG: filename for exclude list: 000_exclude_testuser4.com:8083.conf
DEBUG: loading exclude cache (testuser4.com:8083)
DEBUG: cannot restore exclude cache file (testuser4.com:8083)
DEBUG: init exclude cache (testuser4.com:8083) from file (/usr/local/cwaf/etc
/yml/testuser4.com:8083_exclude.yml)
DEBUG: check integrity of exclude list (testuser4.com:8083)
DEBUG: remove empty exclude file for domain 'testuser4.com:8083'
(000_exclude_testuser4.com:8083.conf)
DEBUG: filename for exclude list: 000_exclude_servername.com:8084.conf
DEBUG: loading exclude cache (servername.com:8084)
DEBUG: cannot restore exclude cache file (servername.com:8084)
DEBUG: init exclude cache (servername.com:8084) from file (/usr/local/cwaf/etc
/yml/servername.com:8084_exclude.yml)
DEBUG: check integrity of exclude list (servername.com:8084)
DEBUG: remove empty exclude file for domain 'servername.com:8084'
(000_exclude_servername.com:8084.conf)
09/07/15 12:25:02 updater[12721]  successful webserver restart
09/07/15 12:25:02 updater[12721]  update successful
09/07/15 12:25:02 updater[12721]  update process finished!
```

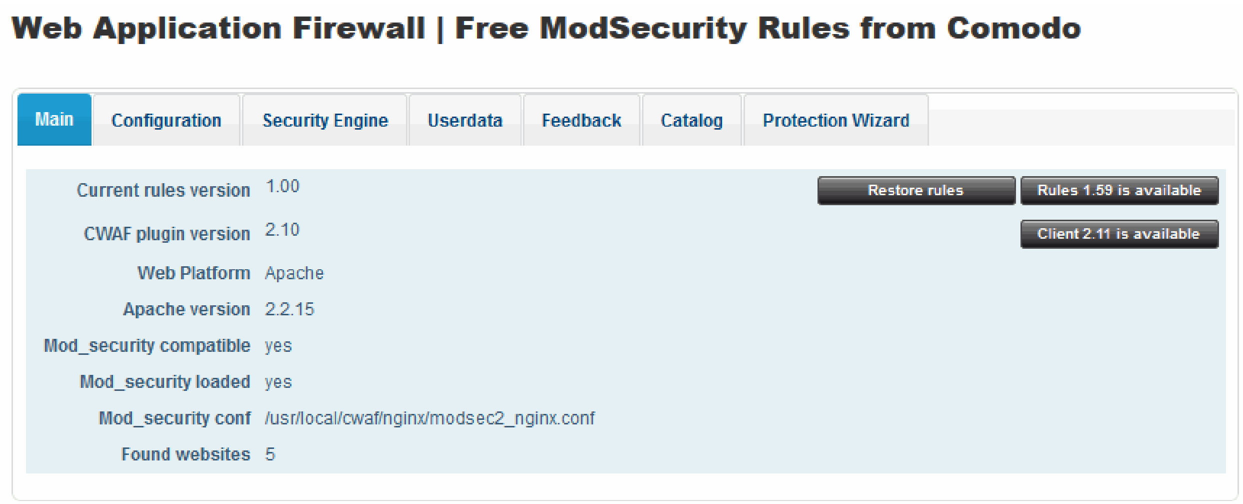
Wait till the page will be reloaded and the last rules will be available.



Current rules version	1.59 (Latest version)
CWAF plugin version	2.10
Web Platform	Apache
Apache version	2.2.15
Mod_security compatible	yes
Mod_security loaded	yes
Mod_security conf	/usr/local/cwaf/nginx/modsec2_nginx.conf
Found websites	5

To update the CWAF plugin to the latest version

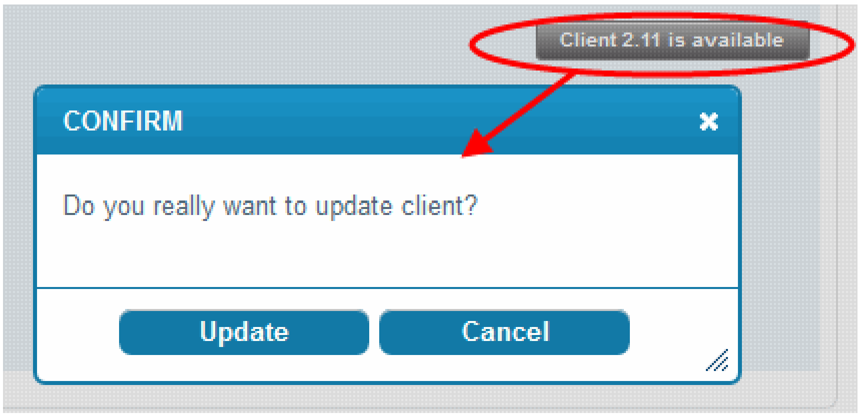
- Login to cPanel on your server
- Click 'Plugins' > "Comodo WAF"
- Click the 'Client X.X is available' at the far right side of the interface



Web Application Firewall | Free ModSecurity Rules from Comodo

Current rules version	1.00
CWAF plugin version	2.10
Web Platform	Apache
Apache version	2.2.15
Mod_security compatible	yes
Mod_security loaded	yes
Mod_security conf	/usr/local/cwaf/nginx/modsec2_nginx.conf
Found websites	5

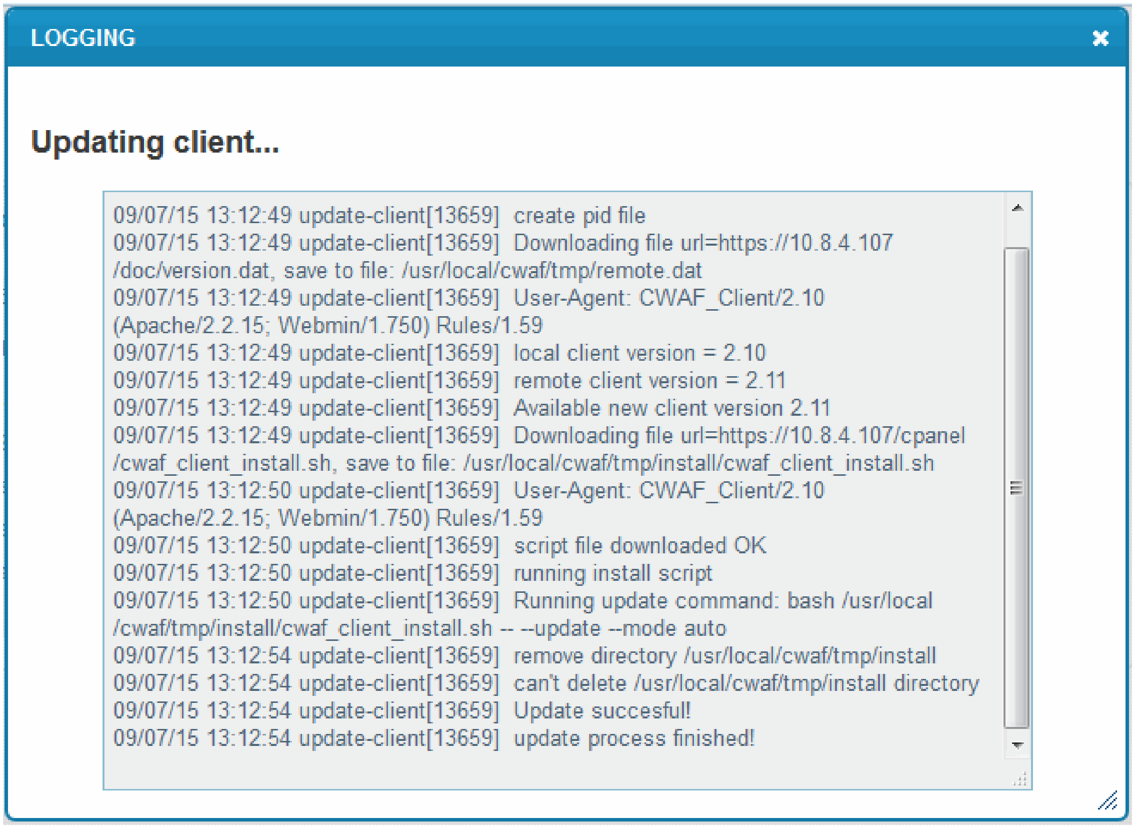
The confirmation message will be displayed.



Do you really want to update client?

Click 'Update'.

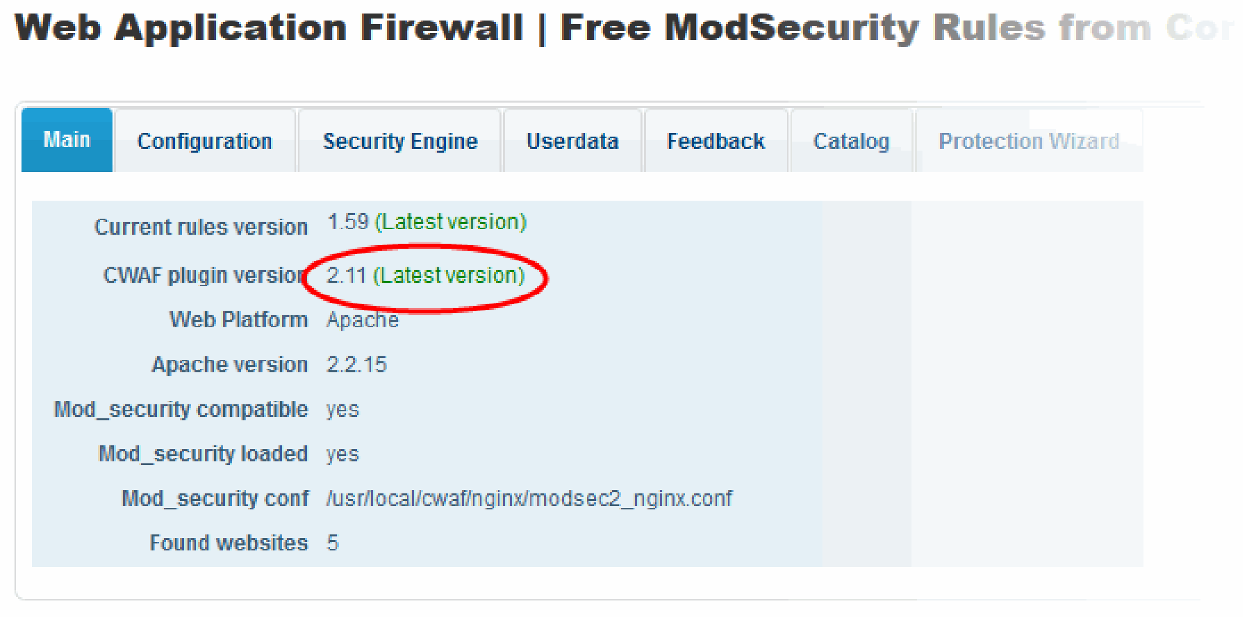
The updater will automatically download and deploy the latest version of plugin.



Updating client...

```
09/07/15 13:12:49 update-client[13659]  create pid file
09/07/15 13:12:49 update-client[13659]  Downloading file url=https://10.8.4.107
/doc/version.dat, save to file: /usr/local/cwaf/tmp/remote.dat
09/07/15 13:12:49 update-client[13659]  User-Agent: CWAF_Client/2.10
(Apache/2.2.15; Webmin/1.750) Rules/1.59
09/07/15 13:12:49 update-client[13659]  local client version = 2.10
09/07/15 13:12:49 update-client[13659]  remote client version = 2.11
09/07/15 13:12:49 update-client[13659]  Available new client version 2.11
09/07/15 13:12:49 update-client[13659]  Downloading file url=https://10.8.4.107/cpanel
/cwaf_client_install.sh, save to file: /usr/local/cwaf/tmp/install/cwaf_client_install.sh
09/07/15 13:12:50 update-client[13659]  User-Agent: CWAF_Client/2.10
(Apache/2.2.15; Webmin/1.750) Rules/1.59
09/07/15 13:12:50 update-client[13659]  script file downloaded OK
09/07/15 13:12:50 update-client[13659]  running install script
09/07/15 13:12:50 update-client[13659]  Running update command: bash /usr/local
/cwaf/tmp/install/cwaf_client_install.sh -- --update --mode auto
09/07/15 13:12:54 update-client[13659]  remove directory /usr/local/cwaf/tmp/install
09/07/15 13:12:54 update-client[13659]  can't delete /usr/local/cwaf/tmp/install directory
09/07/15 13:12:54 update-client[13659]  Update succesful!
09/07/15 13:12:54 update-client[13659]  update process finished!
```

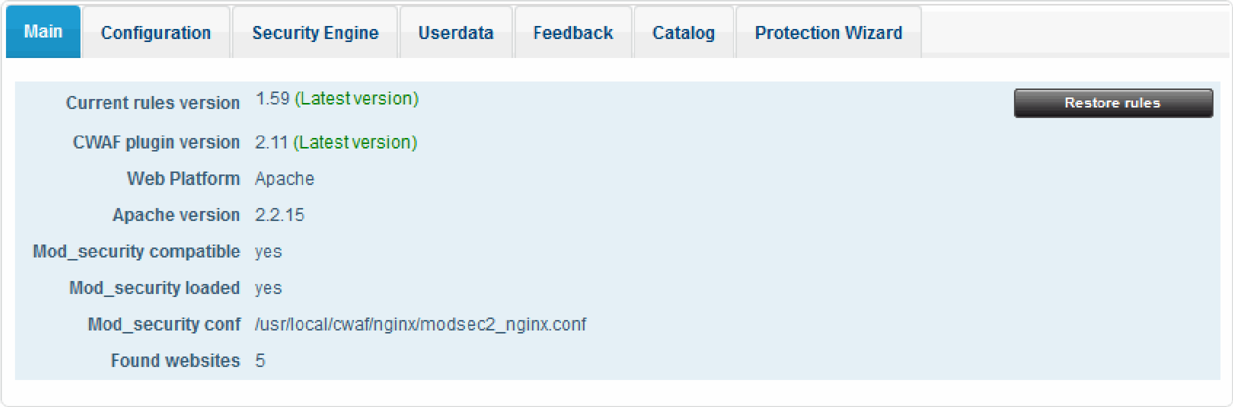
Wait till the page will be reloaded and the last plug-in version will be available.



Current rules version	1.59 (Latest version)
CWAF plugin version	2.11 (Latest version)
Web Platform	Apache
Apache version	2.2.15
Mod_security compatible	yes
Mod_security loaded	yes
Mod_security conf	/usr/local/cwaf/nginx/modsec2_nginx.conf
Found websites	5

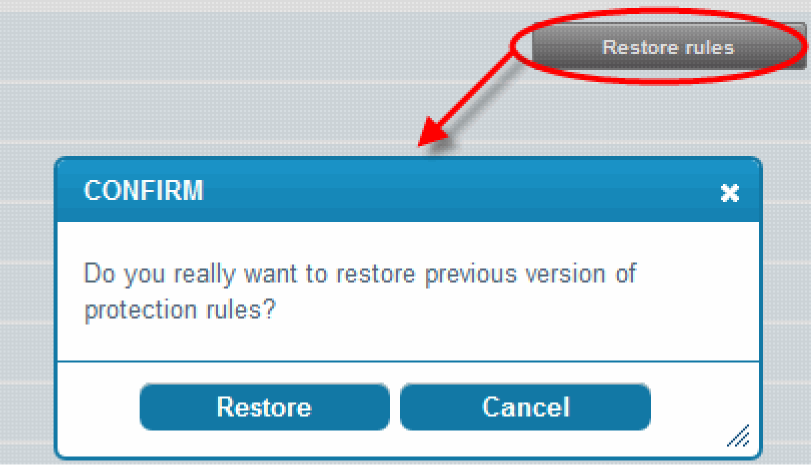
To restore the rule set to the previous version

- Login to cPanel on your server
- Click 'Plugins' > "Comodo WAF"
- Click the 'Restore rules' at the far right side of the interface



Current rules version 1.59 (Latest version)
CWAF plugin version 2.11 (Latest version)
Web Platform Apache
Apache version 2.2.15
Mod_security compatible yes
Mod_security loaded yes
Mod_security conf /usr/local/cwaf/nginx/modsec2_nginx.conf
Found websites 5

The confirmation message will be displayed.



Do you really want to restore previous version of protection rules?

Click 'Restore'.

The agent will revert the last update and restore the previous version of the rule set in the Mod_Security firewall.

You can view the update logs for the details on updates at:

/var/log/CWAF/utils.log

2.1.3.2. Configuring CWAF Parameters

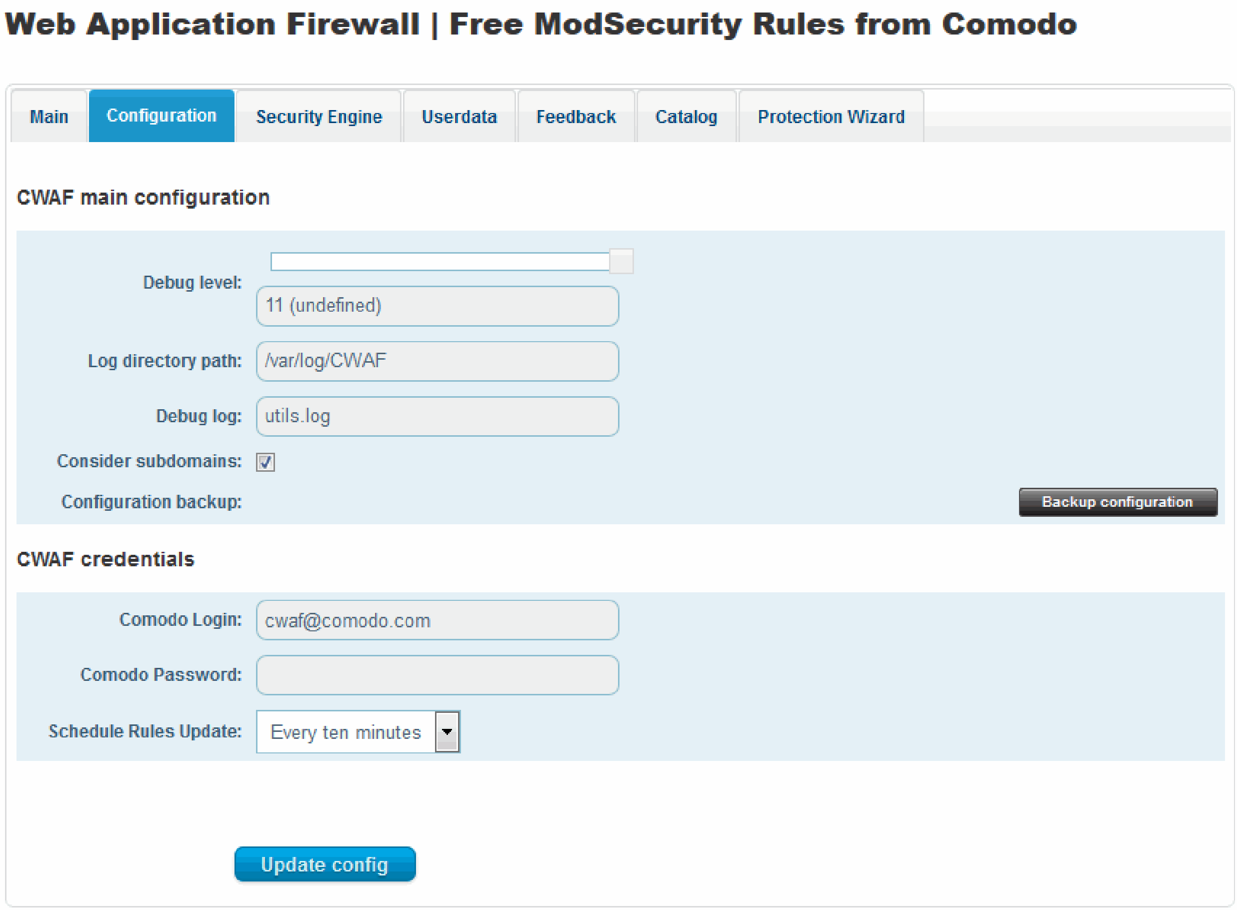
The Configuration tab enables administrators to view and modify various CWAF settings.

CWAF main configuration

- **Debug level** - The slider enables the administrator to set the level of logging the CWAF events. (***Default:*** ***0***)

Level	Description
0	No events will be logged.
1	All critical events will be logged.
2	
3	
4	All Warnings from CWAF will be logged.
5	

6	
7	
8	All Notifications from CWAF will be logged.
9	
10	All the events will be logged.


Web Application Firewall | Free ModSecurity Rules from Comodo

CWAF main configuration

Debug level: 11 (undefined)

Log directory path: /var/log/CWAF

Debug log: utils.log

Consider subdomains: ☑

Configuration backup:

CWAF credentials

Comodo Login: cwaf@comodo.com

Comodo Password:

Schedule Rules Update: Every ten minutes

- **Log directory path** - Enables the administrator to edit the location at which the CWAF log file is stored. (***Default: /var/log/CWAF***)
- **Debug log** - Enables the administrator to specify a name for the log file (***Default: utils.log***)
- **Consider subdomains** - Enables administrators to include/exclude rules of the defined domain and all sub-domains (e.g., *domain.com) along with Catalog operations.
- **Configuration backup –** Enables the administrator to backup user configurations such as: plugin config (debug level, log directory path, login/password etc), userdata files, excluded rules list. From here you can also Restore your configuration.

CWAF credentials

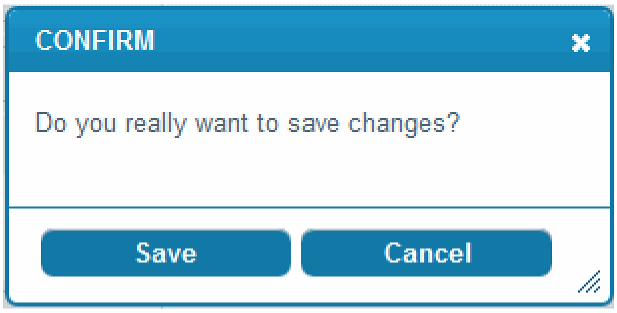
- **Comodo Login** - The login user name for the CWAF account. This field is pre-populated with the userame specified during installation of the agent. If the administrator has changed their login credentials to their CWAF account, they have to specify the latest credentials to enable the agent to log-in to CWAF and download the updated rule sets.
- **Comodo Password** - The login password for the CWAF account. If the administrator has changed their login credentials to their CWAF account, they have to specify the latest credentials to enable the agent to log-in to CWAF

and download the updated rule sets.

Note: For users of DirectAdmin panel, the '**Feedback**' feature will be activated only if the Comodo credentials is set in the above two fields.

- **Schedule Rules Update:** Enables or disables the scheduled rules update. When the schedule is selected from the drop-down box, it will be automatically update certain rules at a specified time. The available scheduling options are: Never, Every ten minutes, Twice an hour, Once an hour, Twice a day, Once a day, Every workday, Twice a week, Once a week, Twice a month and Once a month. Please note that this feature is not available for DirectAdmin panel.

Click the 'Update config' button to save your changes.



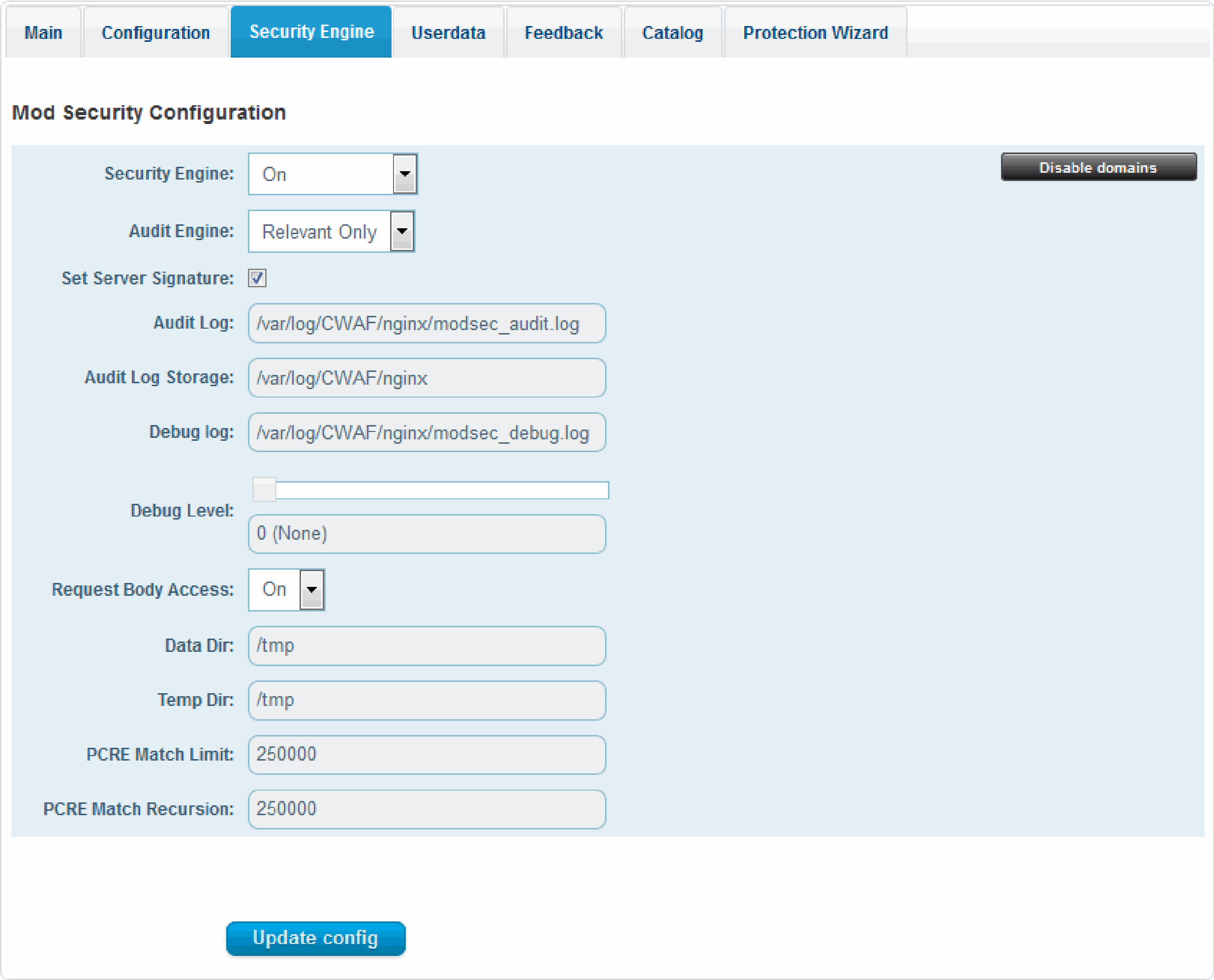
CONFIRM

Do you really want to save changes?

Click 'Save' at the confirmation dialog to save your changes.

2.1.3.3. Managing Security Engine

The 'Security Engine' tab allows you to configure various settings related to your mod_security rules. From here you can also disable mod_security for certain domains.



Mod Security Configuration

Security Engine:	On
Audit Engine:	Relevant Only
Set Server Signature:	☑
Audit Log:	/var/log/CWAF/nginx/modsec_audit.log
Audit Log Storage:	/var/log/CWAF/nginx
Debug log:	/var/log/CWAF/nginx/modsec_debug.log
Debug Level:	0 (None)
Request Body Access:	On
Data Dir:	/tmp
Temp Dir:	/tmp
PCRE Match Limit:	250000
PCRE Match Recursion:	250000

Mod Security Configuration

- **Security Engine**
  - On —Rules are active on the domain
  - Off — Rules are turned off on the domain
  - Detect Only – Rules will detect attacks but will not execute any actions (block, deny, drop, allow, proxy and redirect)
- **Audit Engine** - Enables the administrator to set the behavior of the audit logging engine. (***Default: RelevantOnly).*** *A*vailable options:
  - On - Activates audit logging for all transactions
  - Off - Deactivates audit logging for all transactions
  - Relevant Only – Activates audit logging for transactions that have triggered a warning, error, or have a status code that is considered to be relevant
- **Set Server Signature** - Enabling this checkbox will add SecServerSignature directive to mod_security config. Server response header "Server:" will contain "Protected by COMODO WAF" string instead of the web server version information.
- **Audit Log** – Administrators can modify the path to the main audit log file ***(Default: /usr/local/apache/logs/modsec_audit.log)***
- **Audit Log Storage -** Administrators can modify the path to the audit log storage directory ***(Default: /usr/local/apache/logs/modsec_audit)***
- **Debug log** – Administrators can modify the path to the debug log file ***(Default: /usr/local/apache/logs/modsec_debug.log***)

- **Debug Level** - Set the level of logging the CWAF events. (***Default:* 0**). The following table shows the list of levels:

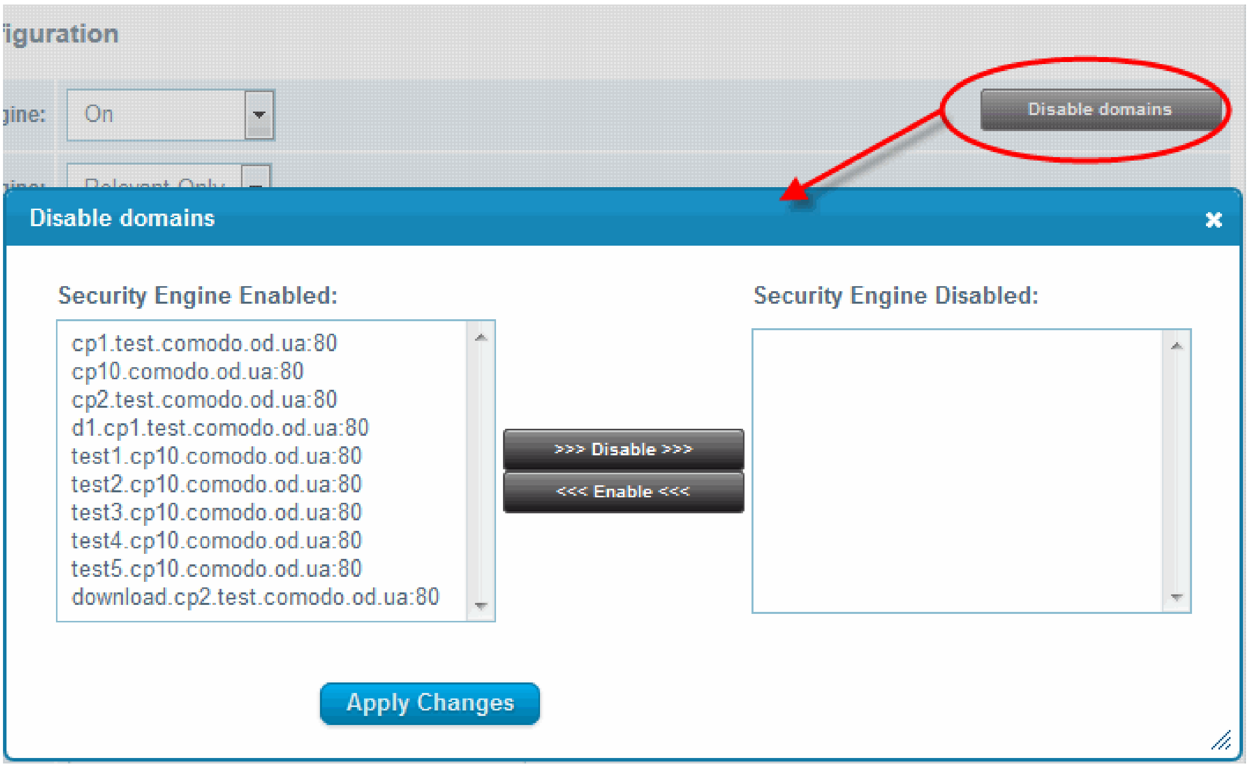
Level	Description
0	No events will be logged.
1	All errors (intercepted requests) will be logged.
2	All Warnings will be logged.
3	All Notifications will be logged.
4	Details of how transactions are handled will be logged.
5	As above but including information about each piece of information handled
6	
7	
8	
9	Log everything, including very detailed debugging information

- **Request Body Access** – Specify whether request bodies will be buffered and processed by mod_security. ***(Default: On)***.
- **Data Dir** – Allows administrators to specify the path to the persistent data (e.g., IP address data, session data, and etc.) ***(Default: /tmp)***
- **Temp Dir** - Enables administrators to specify the directory for temporary files. ***(Default: /tmp)***
- **PCRE Match Limit** – Allows administrators to set limit the maximum amount of memory/time spent trying to match sample text to a pattern in the PCRE library. (***Default: 250000***)
- **PCRE Match Recursion** - Allows administrators to set the match limit recursion in the PCRE library. (***Default: 250000***)

To disable/enable mod_security for individual domains

- Login to cPanel on your server
- Click 'Plugins' > "Comodo WAF".
- Click the 'Disable domains' button at the far right side of the interface

The Disable domains interface will be displayed:

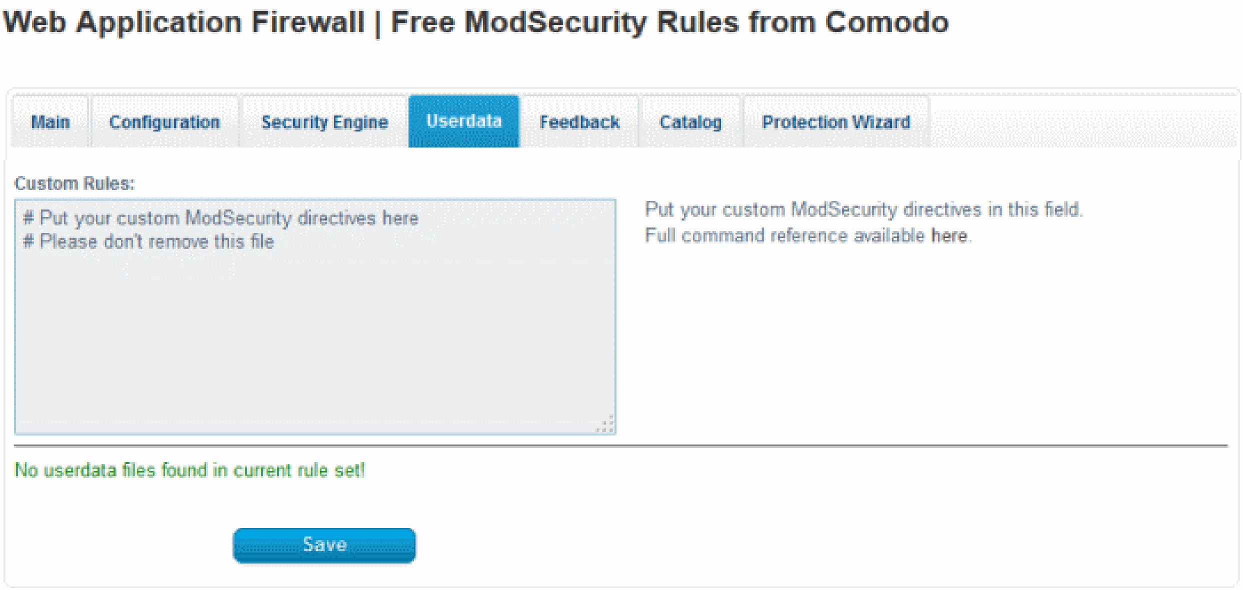

iguration
gine: On
Disable domains
Disable domains
Security Engine Enabled:
cp1.test.comodo.od.ua:80
cp10.comodo.od.ua:80
cp2.test.comodo.od.ua:80
d1.cp1.test.comodo.od.ua:80
test1.cp10.comodo.od.ua:80
test2.cp10.comodo.od.ua:80
test3.cp10.comodo.od.ua:80
test4.cp10.comodo.od.ua:80
test5.cp10.comodo.od.ua:80
download.cp2.test.comodo.od.ua:80
>>> Disable >>>
<<< Enable <<<
Security Engine Disabled:
Apply Changes

- Click on the domain or domains you wish to disable and click the '>>>Disable>>>' button to move it to the 'Disabled' list
- Click "Apply Changes" to save your configuration.
- Restart the server for the settings to take effect.

Note: To disable **all** domains, it is better to use the On/Off switch in the 'Security Engine' page.

2.1.3.4. Configuring Userdata

The Userdata tab contains 'Custom rules' directives for mod_security and custom user rules settings for currently active ruleset.

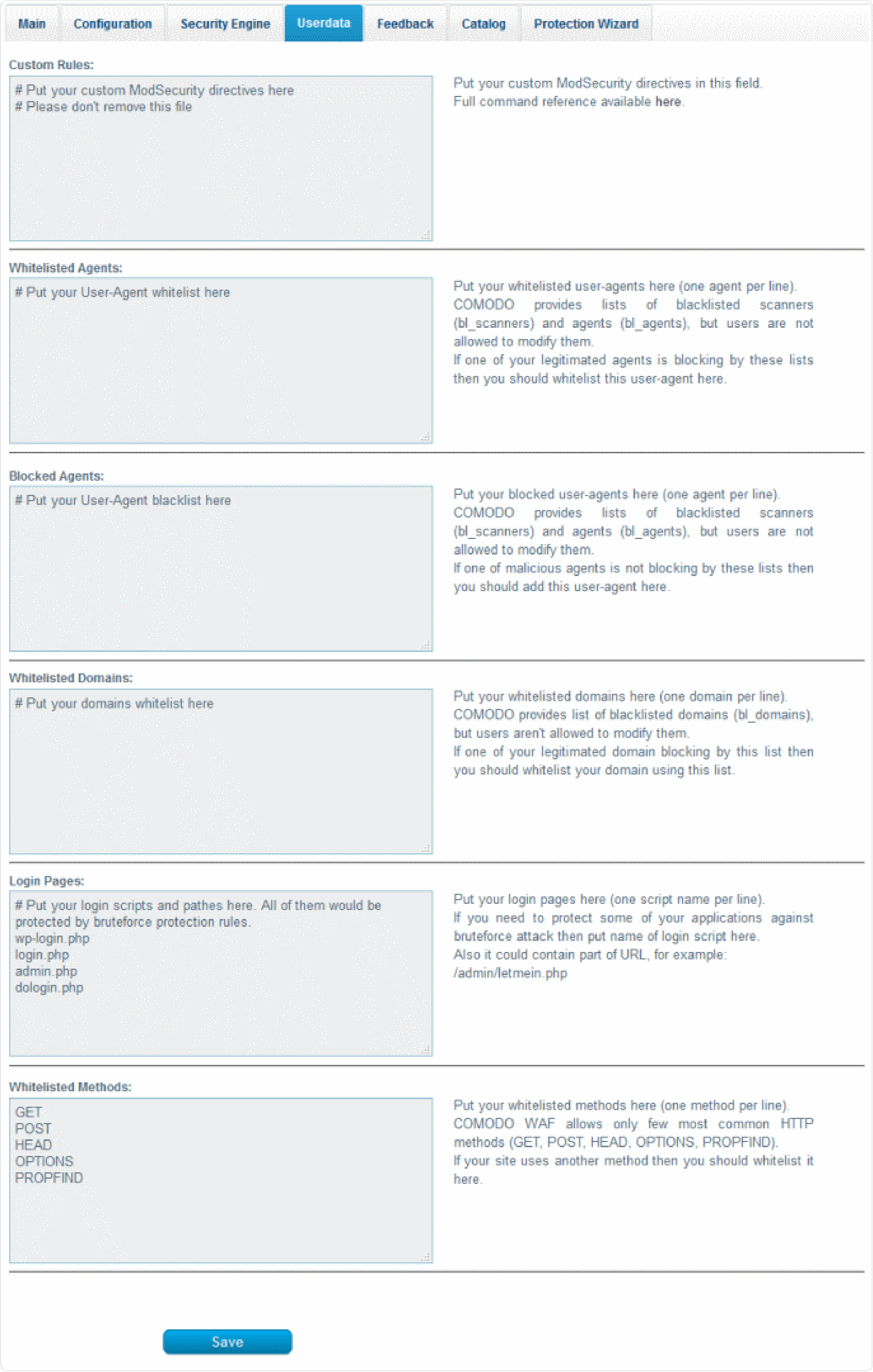


```
# Put your custom ModSecurity directives here
# Please don't remove this file
```

Put your custom ModSecurity directives in this field.
Full command reference available here.

No userdata files found in current rule set!

To add custom user rules settings, download the latest rule set version. Refer to **Viewing and Updating CWAF Information** for more details.



Custom Rules:

```
# Put your custom ModSecurity directives here
# Please don't remove this file
```

Put your custom ModSecurity directives in this field.
Full command reference available here.

Whitelisted Agents:

```
# Put your User-Agent whitelist here
```

Put your whitelisted user-agents here (one agent per line).
COMODO provides lists of blacklisted scanners (bl_scanners) and agents (bl_agents), but users are not allowed to modify them.
If one of your legitimated agents is blocking by these lists then you should whitelist this user-agent here.

Blocked Agents:

```
# Put your User-Agent blacklist here
```

Put your blocked user-agents here (one agent per line).
COMODO provides lists of blacklisted scanners (bl_scanners) and agents (bl_agents), but users are not allowed to modify them.
If one of malicious agents is not blocking by these lists then you should add this user-agent here.

Whitelisted Domains:

```
# Put your domains whitelist here
```

Put your whitelisted domains here (one domain per line).
COMODO provides list of blacklisted domains (bl_domains), but users aren't allowed to modify them.
If one of your legitimated domain blocking by this list then you should whitelist your domain using this list.

Login Pages:

```
# Put your login scripts and pathes here. All of them would be
protected by bruteforce protection rules.
wp-login.php
login.php
admin.php
dologin.php
```

Put your login pages here (one script name per line).
If you need to protect some of your applications against bruteforce attack then put name of login script here.
Also it could contain part of URL, for example:
/admin/letmein.php

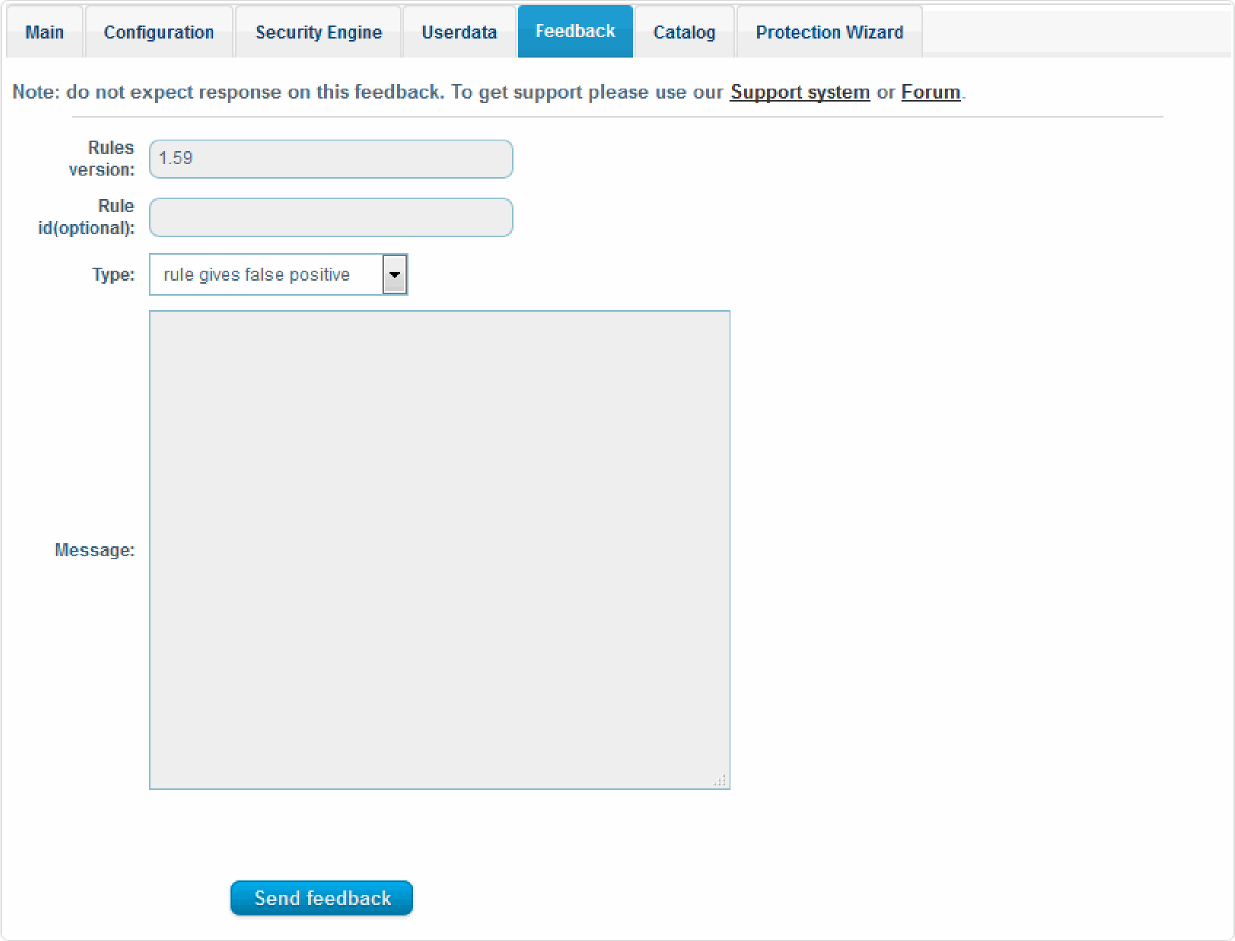
Whitelisted Methods:

```
GET
POST
HEAD
OPTIONS
PROPFIND
```

Put your whitelisted methods here (one method per line).
COMODO WAF allows only few most common HTTP methods (GET, POST, HEAD, OPTIONS, PROPFIND).
If your site uses another method then you should whitelist it here.

2.1.3.5. Sending Feedback

The Feedback tab allows administrators to post feedback on the currently loaded rule set to Comodo. Comodo technicians will consider all suggestions and may be used to correct and enhance the rule set for the next version.



Note: do not expect response on this feedback. To get support please use our Support system or Forum.

Rules version: 1.59

Rule id(optional):

Type: rule gives false positive

Message:

- **Rules version** - The version number of the currently loaded rule set. This field will be auto-populated.
- **Rule id** - Enter the ID number of the specific rule upon which feedback is being provided. This field is optional.
- **Type** - Select the type of the issue to be reported from the drop-down.
- **Message** – Type your feedback in the 'Message' field.

- Click 'Send feedback' to submit your feedback to Comodo.

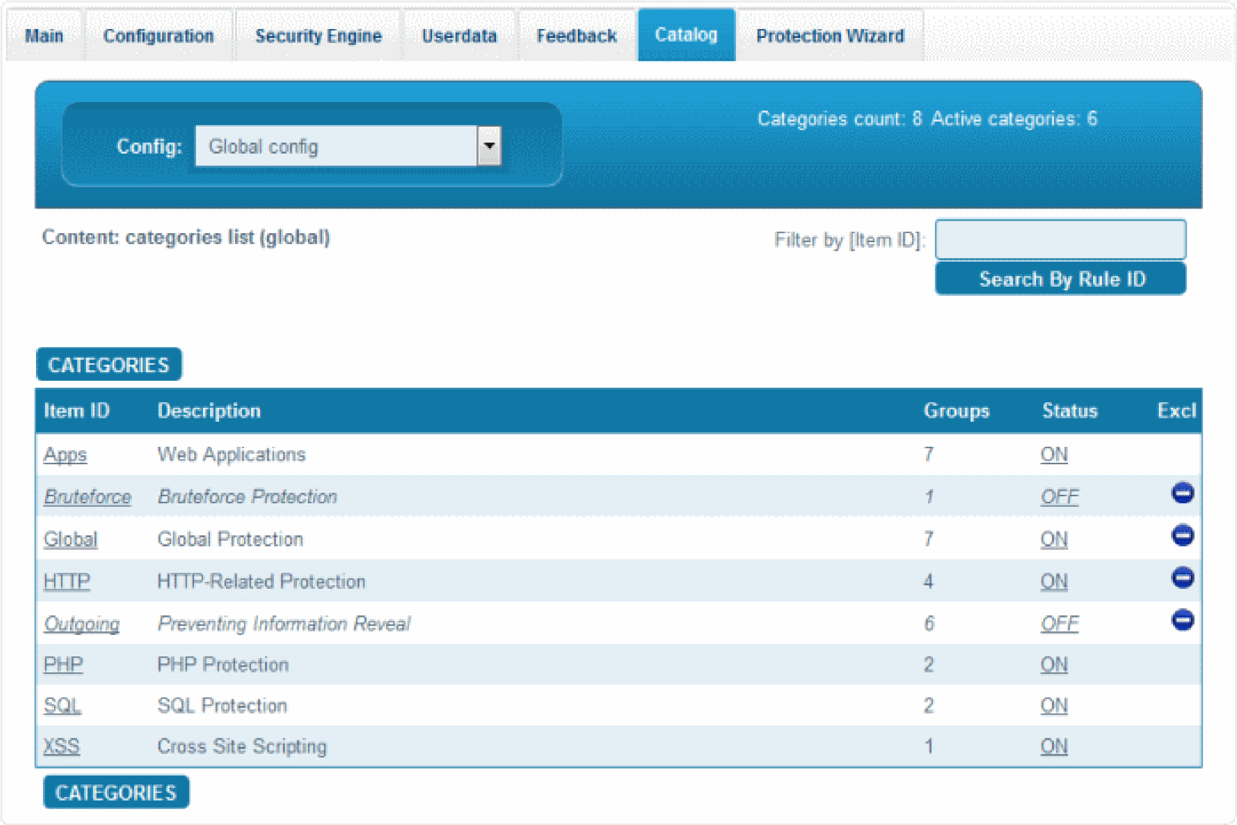
Your feedback is much appreciated. If appropriate, it will implemented in the next update.

Note: For users of DirectAdmin panel, this feature will be activated only if the Comodo credentials is set in the **'Configuration'** section.

2.1.3.6. Managing Catalog

The 'Catalog' tab allows administrators to specify rules that should be excluded from the currently loaded rule set. By default the catalog is empty. In order to operate it download the latest rule set version. The list of domains will be appear after the rule set has been downloaded.

Refer to **Viewing and Updating CWAF Information** for more details.



Config: Global config

Categories count: 8 Active categories: 6

Content: categories list (global)

Filter by [Item ID]:

Item ID	Description	Groups	Status	Excl
Apps	Web Applications	7	ON	
Bruteforce	*Bruteforce Protection*	*1*	*OFF*	⊖
Global	Global Protection	7	ON	⊖
HTTP	HTTP-Related Protection	4	ON	⊖
Outgoing	*Preventing Information Reveal*	*6*	*OFF*	⊖
PHP	PHP Protection	2	ON	
SQL	SQL Protection	2	ON	
XSS	Cross Site Scripting	1	ON	

- Config – Allows administrators to select the scope of catalog operations. Catalog operations can be applied to whole server or per-domain basis.

  Global config – Catalog operations will be performed for whole server. If you wish to apply actions to individual domains, click the arrow in the drop-down box and select the required domain.

The catalog can be managed on three levels: categories, groups and rules. To navigate a level down link in 'Item ID' can be used.

Catalog table contain following columns:

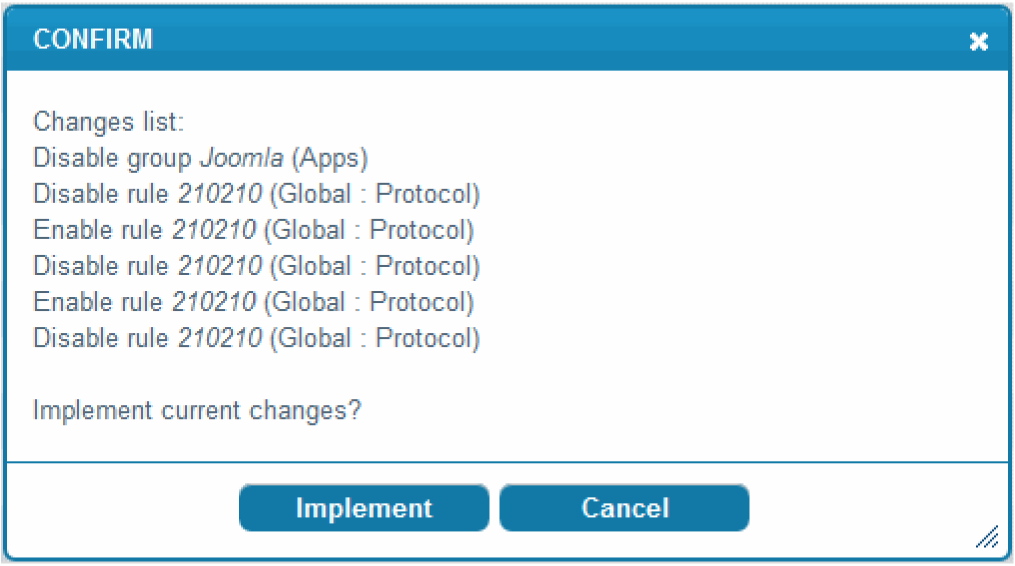
Categories - Column Descriptions		
Column Heading		**Description**
Item ID		The Identity (ID) Number assigned to the rule set. This field can contain the name of a category (on category level), name of group (on group level) or rule ID (on rule level). Click this link to get to the next level down.
Description		Description of the category, group or rule.
Groups		Indicates the amount of groups/rules available for current category/group
Status		Indicates the current status of the item (enabled or disabled). Click this link to enable or disable the item.
Excl		Indicates whether this section contains excluded (disabled) rules. Click the icon to display a list of disabled items in the category or group.
Controls	CATEGORIES, GROUPS, RULES	Enables administrators to move one level up/down in catalog hierarchy

Rules that should not be executed can be excluded from categories/groups

- Blocking item in the 'GROUPS' level, will block all rule defined in that group.

- Blocking an item at the 'RULES' level, will exclude the selected rule ID from the current group.

Click 'Implement' to save settings. A confirmation window will be displayed:



CONFIRM

Changes list:
Disable group *Joomla* (Apps)
Disable rule *210210* (Global : Protocol)
Enable rule *210210* (Global : Protocol)
Disable rule *210210* (Global : Protocol)
Enable rule *210210* (Global : Protocol)
Disable rule *210210* (Global : Protocol)

Implement current changes?

Click 'Implement'.

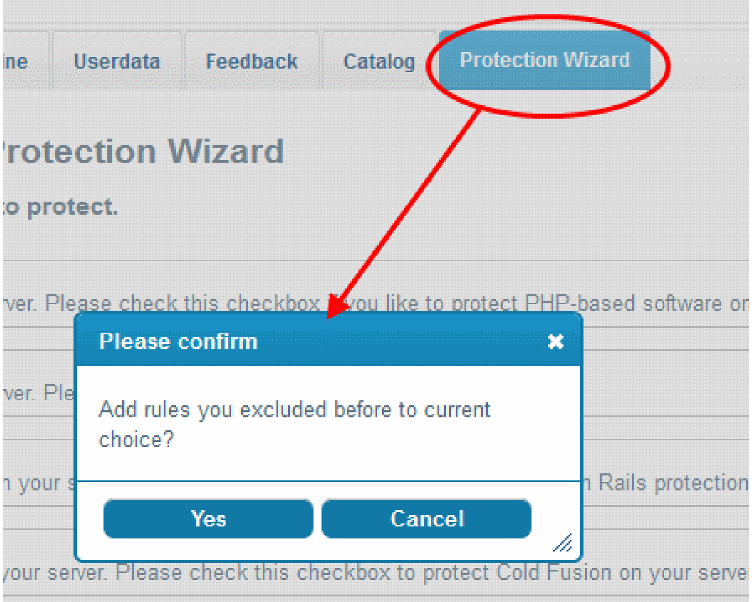
The ⊖ icon will appear next to blocked items. To unblock a rule, click ⊖ again.

Filtering and search options:

- Select the 'Config' drop-down to change scope (Global or Per-domain)
- Start typing in 'Filter by [Item ID]' field to search word or ID number on this page
- Click the 'Search By Rule ID' button to search rule by ID from 'Filter by [Item ID]' field.
- Click ⊖ to get a list of disabled (excluded) rules for this category or group.

2.1.3.7. Protection Wizard

The 'Protection Wizard' tab allows administrators to disable rules affecting web applications that are not installed on your server, thus helping to reduce the server load. Though the functionality of this section is similar to '**Catalog**', the 'Protection Wizard' interface provides at-a-glance view of all categories, groups and rules allowing administrators to create rules depending on the installed applications. Previously excluded rules for a particular category can also be imported here and added to global exclude list. On opening the 'Protection Wizard' screen, administrators can choose to exclude rules which were configured in the '**Catalog**' section.

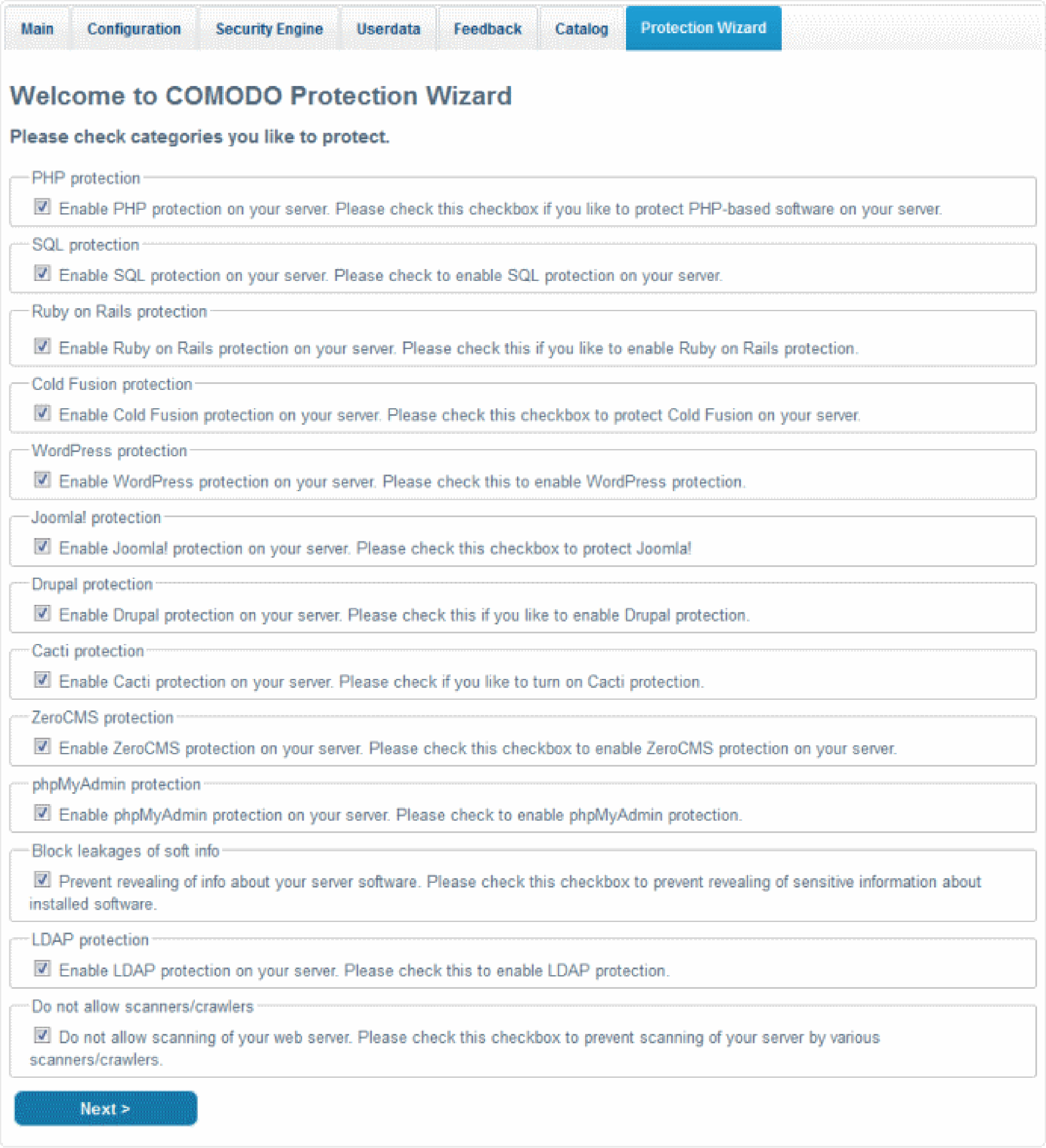


ine
Userdata
Feedback
Catalog
Protection Wizard
rotection Wizard
o protect.
ver. Please check this checkbox if you like to protect PHP-based software on
ver. Ple
n your s
n Rails protection
your server. Please check this checkbox to protect Cold Fusion on your serve

Please confirm

Add rules you excluded before to current choice?

- Click 'Yes' to add rules to be excluded in the Protection Wizard.
- Click 'Cancel' to review the full list and select the rules to be enabled.



Welcome to COMODO Protection Wizard

Please check categories you like to protect.

PHP protection

☑ Enable PHP protection on your server. Please check this checkbox if you like to protect PHP-based software on your server.

SQL protection

☑ Enable SQL protection on your server. Please check to enable SQL protection on your server.

Ruby on Rails protection

☑ Enable Ruby on Rails protection on your server. Please check this if you like to enable Ruby on Rails protection.

Cold Fusion protection

☑ Enable Cold Fusion protection on your server. Please check this checkbox to protect Cold Fusion on your server.

WordPress protection

☑ Enable WordPress protection on your server. Please check this to enable WordPress protection.

Joomla! protection

☑ Enable Joomla! protection on your server. Please check this checkbox to protect Joomla!

Drupal protection

☑ Enable Drupal protection on your server. Please check this if you like to enable Drupal protection.

Cacti protection

☑ Enable Cacti protection on your server. Please check if you like to turn on Cacti protection.

ZeroCMS protection

☑ Enable ZeroCMS protection on your server. Please check this checkbox to enable ZeroCMS protection on your server.

phpMyAdmin protection

☑ Enable phpMyAdmin protection on your server. Please check to enable phpMyAdmin protection.

Block leakages of soft info

☑ Prevent revealing of info about your server software. Please check this checkbox to prevent revealing of sensitive information about installed software.

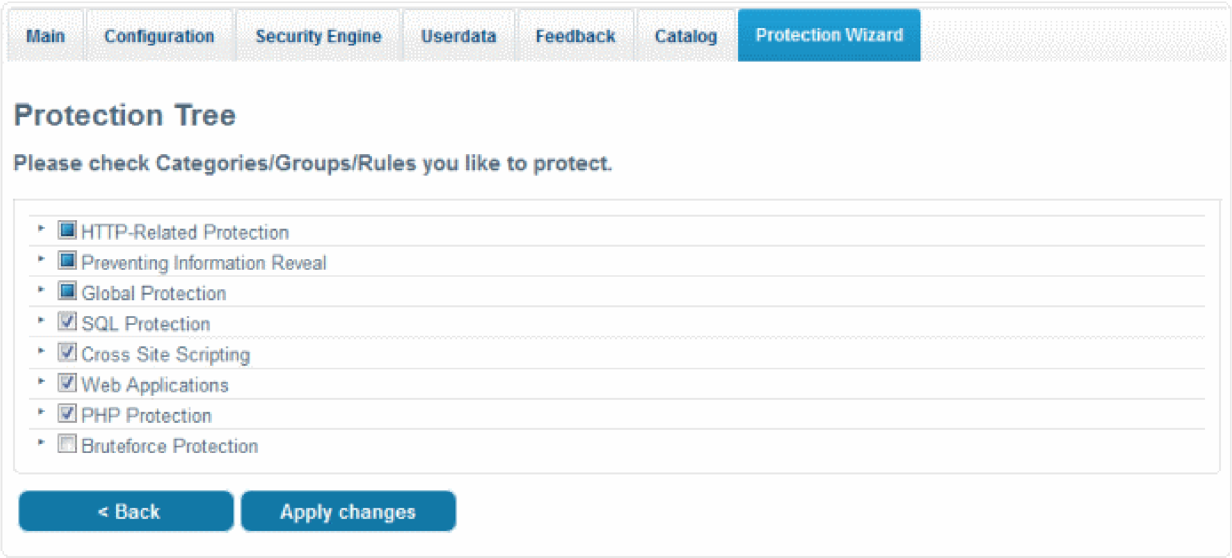
LDAP protection

☑ Enable LDAP protection on your server. Please check this to enable LDAP protection.

Do not allow scanners/crawlers

☑ Do not allow scanning of your web server. Please check this checkbox to prevent scanning of your server by various scanners/crawlers.

By default, all categories are enabled. Clicking the 'Next' button will display the 'Categories', 'Groups' and 'Rules' in a tree structure.

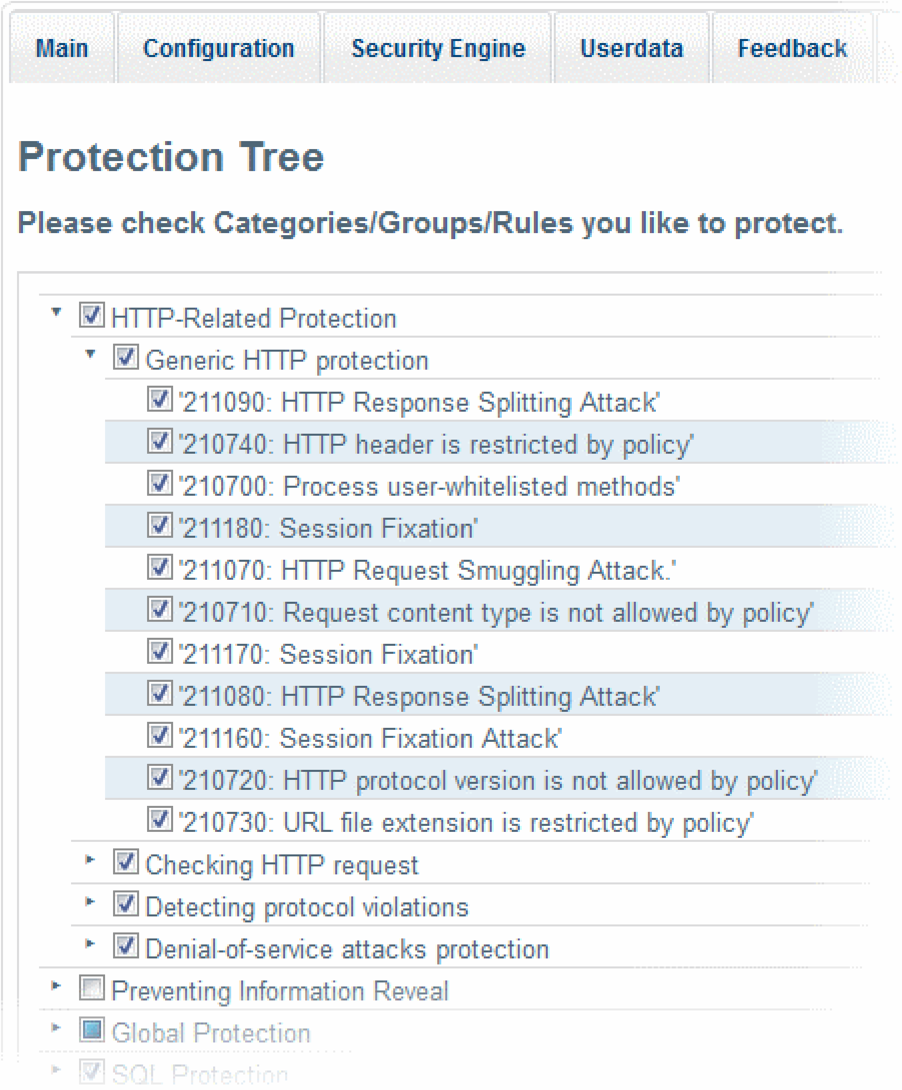


Protection Tree

Please check Categories/Groups/Rules you like to protect.

- ■ HTTP-Related Protection
- ■ Preventing Information Reveal
- ■ Global Protection
- ☑ SQL Protection
- ☑ Cross Site Scripting
- ☑ Web Applications
- ☑ PHP Protection
- □ Bruteforce Protection

- Click on the expand/collapse button ▸ beside a category/group/rule to enable or disable.



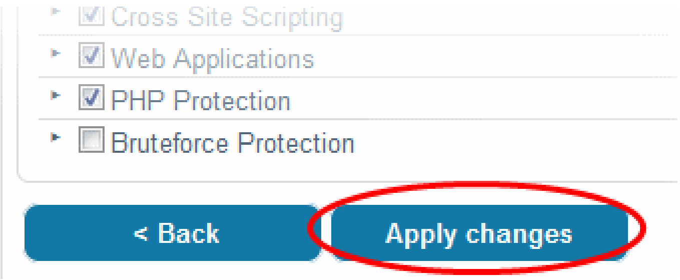
Protection Tree

Please check Categories/Groups/Rules you like to protect.

- ☑ HTTP-Related Protection
  - ☑ Generic HTTP protection
    - ☑ '211090: HTTP Response Splitting Attack'
    - ☑ '210740: HTTP header is restricted by policy'
    - ☑ '210700: Process user-whitelisted methods'
    - ☑ '211180: Session Fixation'
    - ☑ '211070: HTTP Request Smuggling Attack.'
    - ☑ '210710: Request content type is not allowed by policy'
    - ☑ '211170: Session Fixation'
    - ☑ '211080: HTTP Response Splitting Attack'
    - ☑ '211160: Session Fixation Attack'
    - ☑ '210720: HTTP protocol version is not allowed by policy'
    - ☑ '210730: URL file extension is restricted by policy'
  - ☑ Checking HTTP request
  - ☑ Detecting protocol violations
  - ☑ Denial-of-service attacks protection
- □ Preventing Information Reveal
- ■ Global Protection
- ☑ SQL Protection

Please note that if you have selected "Yes' to the option while opening the 'Protection Wizard' screen, the items that were excluded in rules will be automatically be deselected here.

- Select/deselect the items and click the 'Apply changes' button at the bottom.



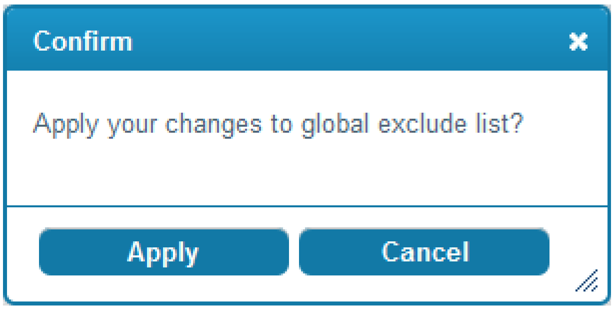
☑ Cross Site Scripting

☑ Web Applications

☑ PHP Protection

□ Bruteforce Protection

- Click the 'Apply' button in the confirmation dialog to apply the changes to global exclude list.



Confirm

Apply your changes to global exclude list?

2.1.4. Using the Agent for Firewall Configuration

The agent installed on the server enables the administrator to manually download and deploy the latest version of the Firewall Rule Sets.

To update the rule set to the latest version, run the CWAF console tool (assuming Agent was installed to /opt/cwaf):

/opt/cwaf/scripts/updater.pl

You can view the update logs for the details on updates at:

/var/log/CWAF/utils.log

To check agent version, installed and available rules version and web platform run:

/opt/cwaf/scripts/updater.pl -v

To update agent to the latest version, run CWAF console tool (if Agent was installed at /opt/cwaf):

/opt/cwaf/scripts/update-client.pl

To check agent version, last available agent version and web platform run:

/opt/cwaf/scripts/update-client.pl -v

The administrator can assign these scripts to be run periodically as Cron jobs. To get more information refer to “How to set up a Cron job” section in your operation system manual.

The command line tool for protection rules management is supported for client agent version 2.3 and above. Refer to the next section **'Command Line Utility'** for more details.

2.1.5. Command Line Utility

New command-line utilities from Client version 2.3 and above is now supported for protection rule management that includes the following:

- Turn on/off all protection rules (mod_security) for domain.
- Enable/disable rules by ID for domain.

Usage:

```
./cwaf-cli.pl [arguments]
```

Arguments:

```
-h, --help        - this help message

-g, --loglevel    - set loglevel (1 - 10)

-v, --version     - show client version

-l, --domain_list  - show list of domains

-f, --force_domain - apply domain even if it not found
```

Exclude rules:

```
-d,   --domain - set domain for exclude operation (global exclude list if not specified)

-xa,  --exclude_add [rule_ID1 rule_ID2...]  - add rules to exclude list

-xac, --exclude_add_cat [cat1 cat2...]      - add categories to exclude list

-xag, --exclude_add_grp [grp1 grp2...]      - add groups to exclude list

-xd,  --exclude_del [rule_ID1 rule_ID2...]  - remove rules from exclude list

-xdc, --exclude_del_cat [cat1 cat2...]      - remove categories from exclude list

-xdg, --exclude_del_grp [grp1 grp2...]      - remove groups from exclude list

-xl,  --exclude_list                        - show list of excluded rules

-lc,  --list_categories                     - show list of categories

-lg,  --list_groups                         - show list of groups
```

Disable/enable mod_security for domains:

```
-dd, --disable_domain [domain1 domain2...] - disable mod_security for domains

-de, --enable_domain [domain1 domain2...]  - enable mod_security for domains

-dl, --disabled_list                       - show list of disabled domains
```

Examples:

Global disable of the rules by IDs: 230000, 230010

```
./cwaf-cli.pl  -ea 230000 230010
```

Enable rule ID 210700 for domain "mydomain.com:8080"

```
./cwaf-cli.pl  -ed 210700 -d mydomain.com:8080
```

Notes:

- Command-line utilities located in script directory inside of CWAF install tree.
- Domain name should be specified as it looks in plugin or result of "--domain_list" command
- Use --force_domain to perform operations with domains not listed in --domain_list

2.1.6. Uninstalling CWAF

Comodo Web Application Firewall is installed at the following default locations:

- */var/cpanel/cwaf* for cPanel plug-in
- */usr/local/cwaf* for Plesk, DirectAdmin, Webmin plug-in.

The uninstall path for standalone agent was defined by the administrator during installation of the agent.

To uninstall CWAF for cPanel

- Run the script '*bash /var/cpanel/cwaf/scripts/uninstall_cwaf.sh'*

  You will be asked:

  Do you want to remove Comodo WAF application from cPanel?

  Enter answer [y/n] y

To uninstall CWAF for DirectAdmin

- Run the script *'bash /usr/local/cwaf/scripts/uninstall_cwaf.sh'*

You will be asked:

Do you want to remove Comodo WAF application from DirectAdmin?

Enter answer [y/n] y

To uninstall CWAF for Plesk

- Run the script '*bash /usr/local/cwaf/scripts/uninstall_cwaf.sh'*

  You will be asked:

  Do you want to remove Comodo WAF application from Plesk?

  Enter answer [y/n] y

To uninstall CWAF for Webmin

- Run the script 'bash /usr/local/cwaf/scripts/uninstall_cwaf.sh'

  You will be asked:

  Do you want to remove Comodo WAF application from Webmin?

  Enter answer [y/n] y

To uninstall CWAF Agent (*standalone mode)*

- Run the script '*bash <CWAF_INSTALL_PATH>/scripts/uninstall_cwaf.sh*'

  You will be asked:

  Do you want to remove Comodo WAF application?

  Enter answer [y/n] y

  Please don't forget to remove string "Include /opt/cwaf/etc/cwaf.conf" from file /etc/apache2/conf.d/modsec2.conf and reload Apache. To do this:

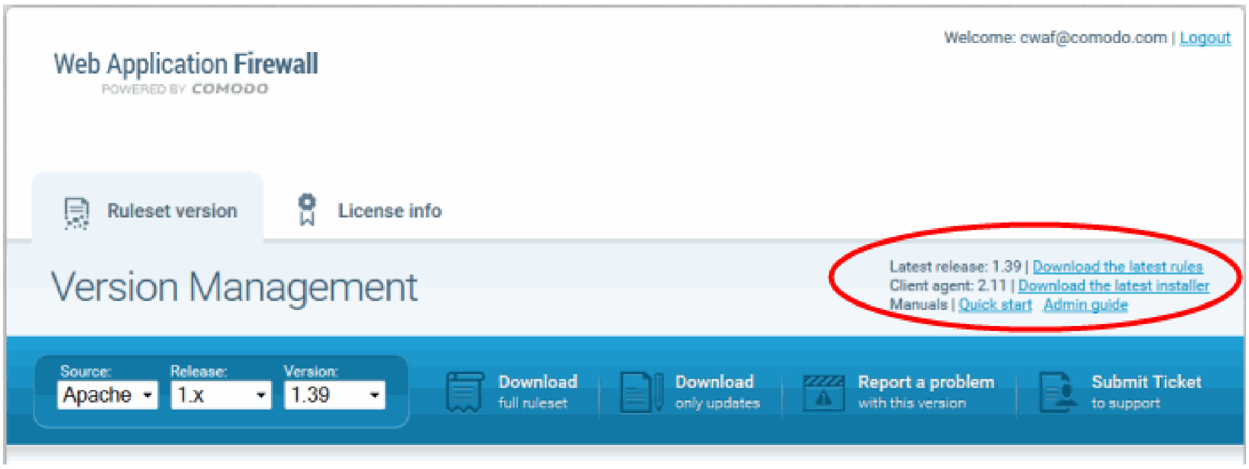
  - Remove the string '*include /opt/cwaf/etc/cwaf.conf*' from the file '*/etc/apache2/conf/modsec2.conf*'
  - Reload 'Apache'

The agent will be removed from the server.

2.2. Downloading and Installing Rule Set Packages

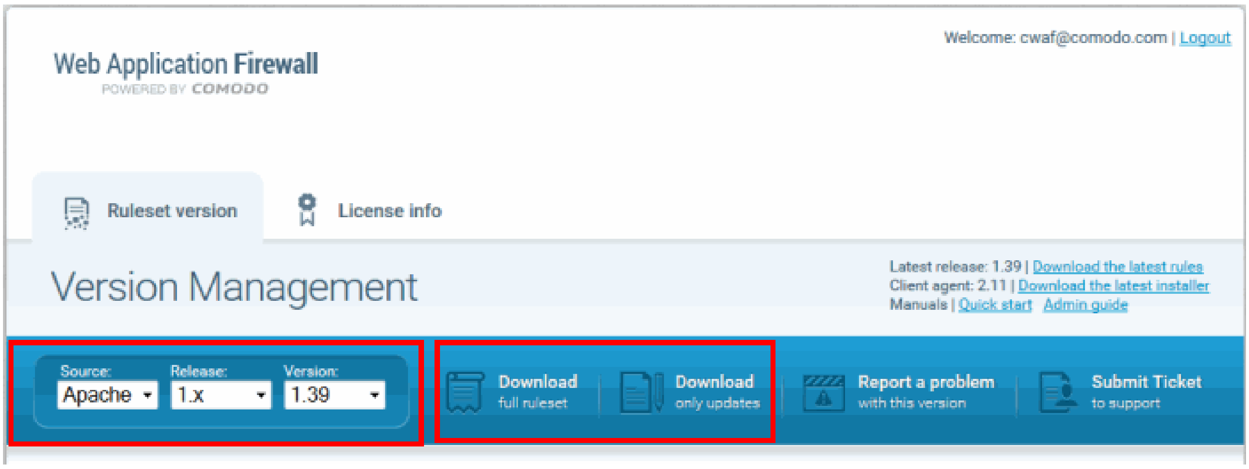
To download the Rule Set

- Log-in to the web administration console at **https://waf.comodo.com**
- Ensure that the 'Rule set version' tab is opened
- If you want to download the latest version directly, click the 'Download latest rules set' shortcut link at the top right


Web Application Firewall
POWERED BY COMODO
Welcome: cwaf@comodo.com | Logout
Ruleset version
License info
Version Management
Latest release: 1.39 | Download the latest rules
Client agent: 2.11 | Download the latest installer
Manuals | Quick start Admin guide
Source: Apache
Release: 1.x
Version: 1.39
Download full ruleset
Download only updates
Report a problem with this version
Submit Ticket to support

- If you want to download a selected version of the rule set,
  - Select the version from the 'Select version' drop-down
  - Select the release number from the 'Select release' drop-down

The rule sets contained in the selected version of the package will be listed under 'List of rule files', along with its release date and time.



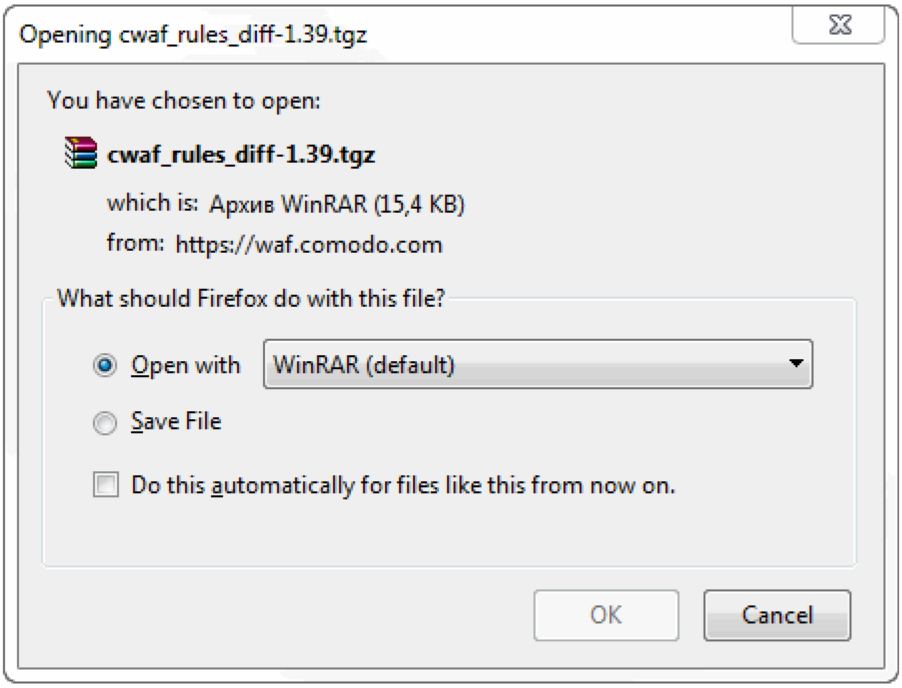
Welcome: cwaf@comodo.com | Logout

Latest release: 1.39 | Download the latest rules
Client agent: 2.11 | Download the latest installer
Manuals | Quick start Admin guide

Source: Apache
Release: 1.x
Version: 1.39

- If you are installing the rule set for the first time, click 'Download full rules set' to download the full set of the selected version.
- If you have already installed the previous version of the rule set and want to update it to the latest version, click 'Download only updates'

The download dialog will be displayed.



Opening cwaf_rules_diff-1.39.tgz

You have chosen to open:

cwaf_rules_diff-1.39.tgz

which is: Архив WinRAR (15,4 KB)

from: https://waf.comodo.com

What should Firefox do with this file?

● Open with WinRAR (default)

○ Save File

□ Do this automatically for files like this from now on.

- Click 'Save' to save the compressed rule set package file in gzip file format (.tgz) format in a local drive.

To implement the firewall rule sets on to the server

- Extract the rule set package files and transfer them to a local server folder E.g. */opt/comodo/waf*
- Modify Apache Web Server configuration to enable 'mod_security' module and include CWAF Rules.

  E.g. for CentOs system edit the file */etc/httpd/conf.d/mod_security.conf:, to* include the following configuration key:

  Include /opt/comodo/waf/etc/cwaf.conf
- Restart the Apache service.

The rule sets in the package will be implemented immediately.

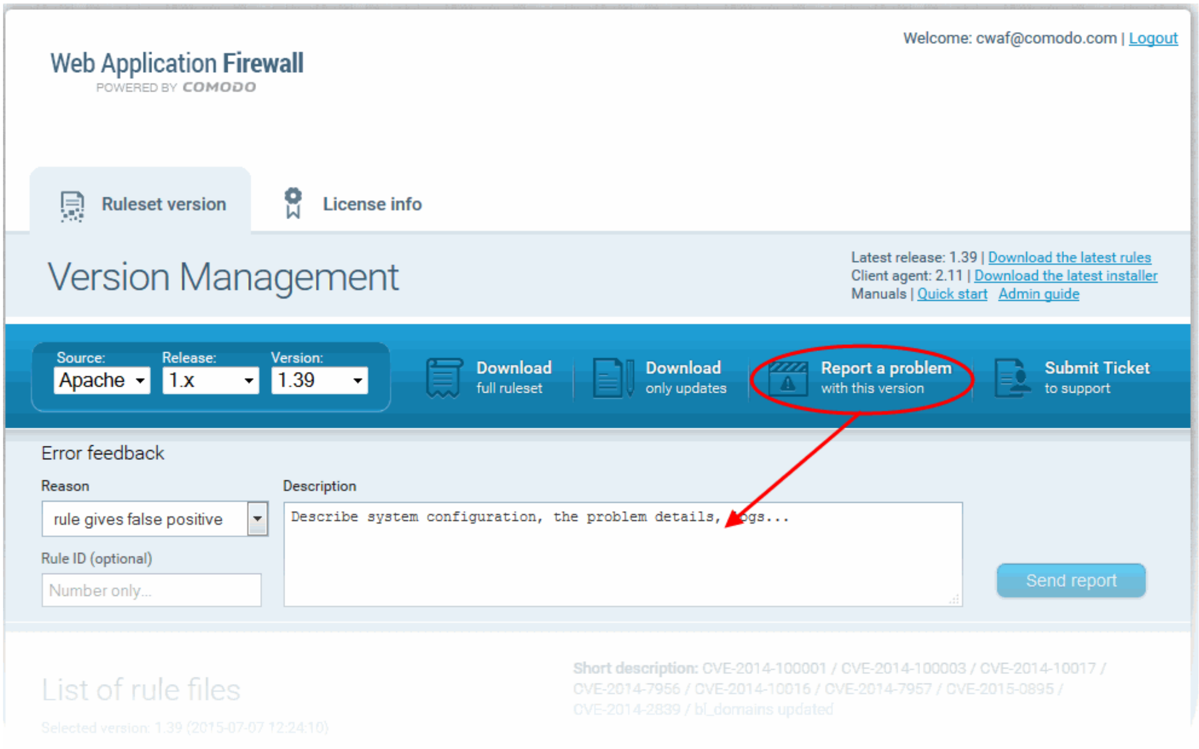
If you want to view or download the CWAF help guide, click the 'Manual' shortcut link at the top right.

2.3. Reporting Problems to Comodo

Customer feedback plays a key role in developing and improving Comodo Web Application Firewall. The 'Report a problem' feature enables administrators to post feedback and report problems on the currently loaded rule set and to notify us of any false positives.

To submit feedback

- Click the 'Report a problem' button at the upper right of the interface:



Latest release: 1.39 | Download the latest rules
Client agent: 2.11 | Download the latest installer
Manuals | Quick start Admin guide

Source: Apache Release: 1.x Version: 1.39

Reason: rule gives false positive

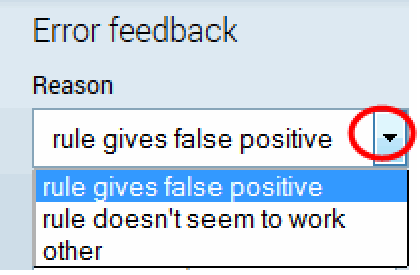
Description: Describe system configuration, the problem details, logs...

Rule ID (optional): Number only...

Short description: CVE-2014-100001 / CVE-2014-100003 / CVE-2014-10017 / CVE-2014-7956 / CVE-2014-10016 / CVE-2014-7957 / CVE-2015-0895 / CVE-2014-2839 / bl_domains updated

Selected version: 1.39 (2015-07-07 12:24:10)

- **Reason** - Choose a subject for your feedback from the drop down menu.
- **Rule ID** - Administrators can enter the ID number of the specific rule upon which feedback is provided. This field is optional.
- **Description** - Enter a description of the problem. If possible, please also provide system configuration details and event logs along with details of the problem.



Error feedback
Reason
rule gives false positive
rule gives false positive
rule doesn't seem to work
other

Click 'Send report' to submit to Comodo.

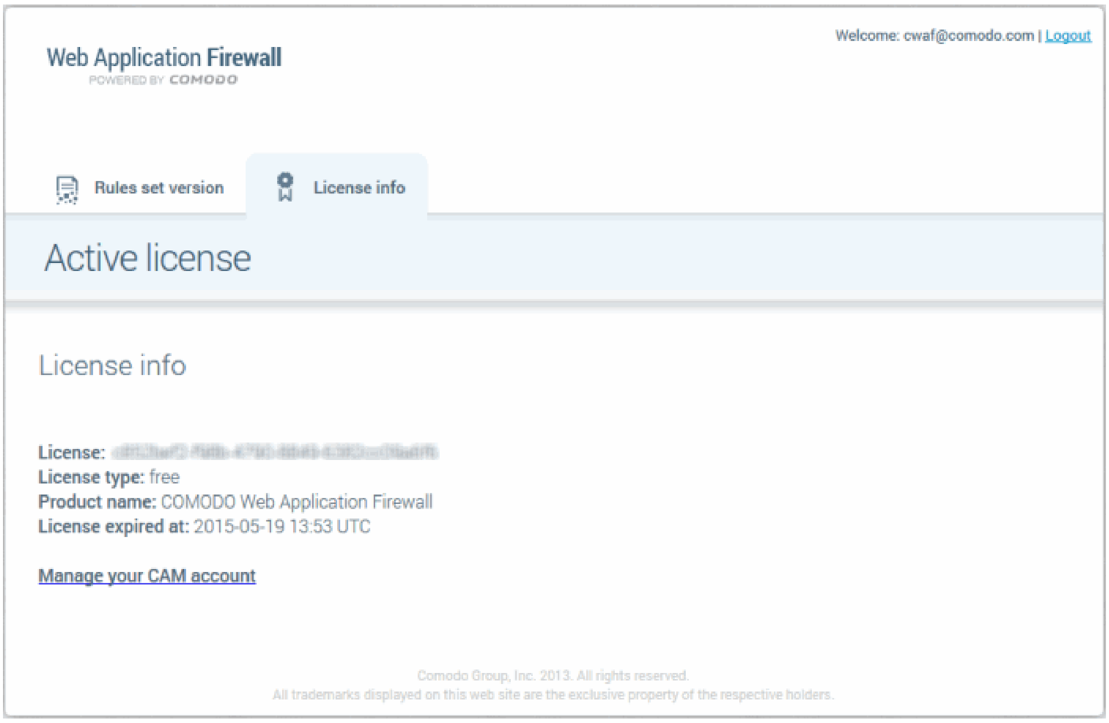
2.4. Submitting Tickets to Comodo

To submit a support ticket

- Click the 'Submit a Ticket' button at the top-right of the interface
- Select 'WAF Support' then click 'Next'
- Select a priority, create a subject for your ticket and describe your problem
- Click 'Submit'.

3. Managing CWAF License

You can view license information from the 'License Info' tab. The interface also provides a shortcut to login to your Comodo Accounts Manager (CAM) account should you need to renew or upgrade your license.



License info

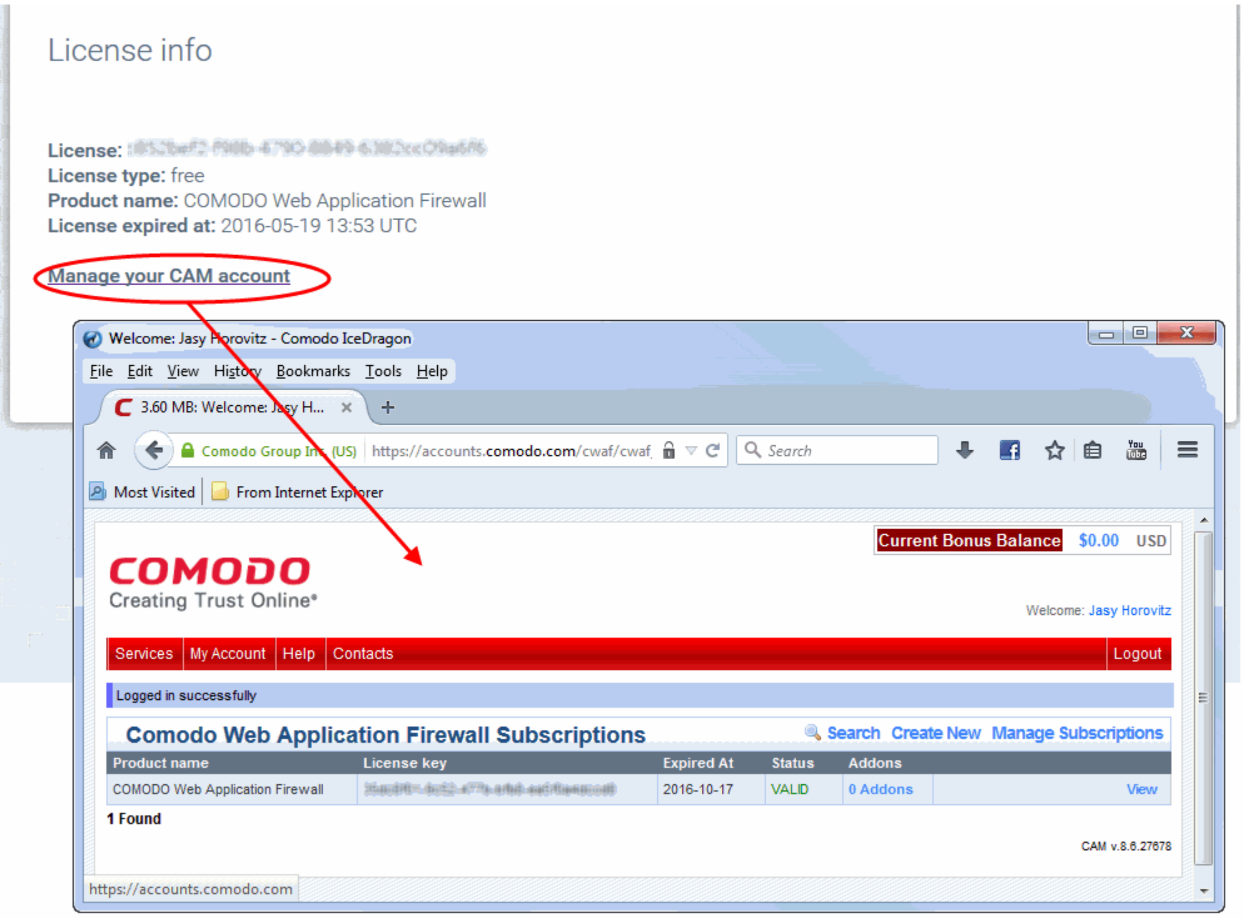
License: [redacted]
License type: free
Product name: COMODO Web Application Firewall
License expired at: 2015-05-19 13:53 UTC

Manage your CAM account

Comodo Group, Inc. 2013. All rights reserved.
All trademarks displayed on this web site are the exclusive property of the respective holders.

- **License** - Displays the account license key.
- **License type:** Displays the type of license - free or paid.
- **Product name** - Displays the name of the product for which you have a license.
- **License expired at** - Displays the expiration date of the license.
- **Manage your CAM account** - Takes you to your account pages at **https://accounts.comodo.com**. The CAM interface allows you to renew or upgrade your license and to subscribe to other Comodo products and services.

  For more guidance on renewing your license and subscribing for other products, please refer to the Comodo Accounts Manager online help guide at **http://help.comodo.com/topic-211-1-513-5907—Introduction-To-Comodo-Accounts-Manager.html**.



License info

License: [redacted]
License type: free
Product name: COMODO Web Application Firewall
License expired at: 2016-05-19 13:53 UTC

Manage your CAM account

Welcome: Jasy Horovitz - Comodo IceDragon
File Edit View History Bookmarks Tools Help
3.60 MB: Welcome: Jasy H...
Comodo Group Inc (US)
https://accounts.comodo.com/cwaf/cwaf
Search
Most Visited
From Internet Explorer
COMODO
Creating Trust Online®
Services
My Account
Help
Contacts
Logout
https://accounts.comodo.com

Current Bonus Balance $0.00 USD

Welcome: Jasy Horovitz

Logged in successfully

Comodo Web Application Firewall Subscriptions — Search Create New Manage Subscriptions

Product name	License key	Expired At	Status	Addons	
COMODO Web Application Firewall	[redacted]	2016-10-17	VALID	0 Addons	View

1 Found

CAM v.8.6.27678

Appendix 1 - Identifying Rule IDs for Exclusion

The administrator may wish to exclude some rules from the currently loaded rule set for various reasons, including:

- The administrator does not need the protection offered by a specific rule for their web application
- The rule is working incorrectly for their web sites

The rules to be excluded can be added to an exclusion list through the CWAF plug-in by specifying their rule IDs.

Please refer to the section **Using the Web Hosting Control Panel plugin for Firewall Configuration** > '**Managing Catalog**' for more details.

This section explains how to identify the Rule IDs of rules you want to exclude:

Step 1 – Identify the rule ID

To exclude a rule that is not needed (cPanel)

- Navigate to the directory */var/cpanel/cwaf/rules/* where rulefiles are stored and identify the rule(s) to be excluded.
- Open the rule file.

  Example:

  The rule file '*/var/cpanel/cwaf/rules/cwaf_05.conf*' is shown below:

  ```
  SecRule REQUEST_HEADERS:Cookie "@rx (^|;)=(;|$)" \
      "id:220020,\
      msg:'COMODO WAF: found CVE-2012-0021 attack',\
      phase:1,\
      deny,\
      status:403,\
      log"
  ```
- Get the rule ID from the string.

  In the example above, the rule ID is '*220020*'

To exclude a rule that is not needed (Plesk)

- Navigate to the directory */usr/local/cwaf/rules/* where rulefiles are stored and identify the rule(s) to be excluded.
- Open the rule file.

  Example:

  The rule file '/usr/local/cwaf/rules/*cwaf_05.conf*' is shown below:

  ```
  SecRule REQUEST_HEADERS:Cookie "@rx (^|;)=(;|$)" \
      "id:220020,\
      msg:'COMODO WAF: found CVE-2012-0021 attack',\
      phase:1,\
      deny,\
      status:403,\
      log"
  ```
- Get the rule ID from the string.

  In the example above, the rule ID is '*220020*'

To exclude a rule that is not needed (standalone mode)

- Navigate to the directory *'/opt/cwaf/etc/cwaf/'* where rulefiles are stored and identify the rule(s) to be excluded.
- Open the rule file.

  Example:

  The rule file *"opt/cwaf/etc/cwaf/cwaf_05.conf'* is shown below:

  ```
  SecRule REQUEST_HEADERS:Cookie "@rx (^|;)=(;|$)" \
      "id:220020,\
      msg:'COMODO WAF: found CVE-2012-0021 attack',\
      phase:1,\
      deny,\
      status:403,\
      log"
  ```

- Get the rule ID from the string.

  In the example above, the rule ID is '*220020*'

Alternatively, if you find a rule is behaving incorrectly for your web site, such as blocking certain web pages, you can identify the rule and extract the ID from the Mod_Security audit log available at */etc/httpd/logs/modsec_audit.log.*

Example:

```
Message: Access denied with code 403 (phase 2). Pattern match "(?:< ?script ..... [id "80148"] ... [severity "CRITICAL"]
```

In the example above the rule ID is “80148”

Step 2 – Exclude the rule

Use this ID to add the rule to the exclusion list, as explained in the section **Using the Web Hosting Control Panel plugin for Firewall Configuration** > '**Managing Catalog**

Administrators can specify a single rule, a list of rules or a range of rules to be excluded.

About Comodo

The Comodo companies are leading global providers of Security, Identity and Trust Assurance services on the Internet. Comodo CA offers a comprehensive array of PKI Digital Certificates and Management Services, Identity and Content Authentication (Two-Factor - Multi-Factor) software, and Network Vulnerability Scanning and PCI compliance solutions. In addition, with over 10,000,000 installations of its threat prevention products, Comodo Security Solutions maintains an extensive suite of endpoint security software and services for businesses and consumers.

Continual innovation, a core competence in PKI and a commitment to reversing the growth of Internet-crime distinguish the Comodo companies as vital players in the Internet's ongoing development. Comodo, with offices in the US, UK, China, India, Romania and the Ukraine, secures and authenticates the online transactions and communications for over 200,000 business customers and millions of consumers, providing the intelligent security, authentication and assurance services necessary for trust in on-line transactions.

Comodo Security Solutions, Inc.

1255 Broad Street

Clifton, NJ 07013

United States

Tel: +1.877.712.1309

Tel: +1.703.637.9361

Email: **EnterpriseSolutions@Comodo.com**

For additional information on Comodo - visit **http://www.comodo.com.**