



**COMODO**  
Creating Trust Online®

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

# Comodo

# Web Application Firewall

Software Version 2.17

**Administrator Guide**  
Guide Version 2.17.061118

Comodo Security Solutions  
1255 Broad Street  
Clifton, NJ 07013

## Table of Contents

<b>1. Comodo Free ModSecurity Rules - Introduction</b> .....	<b>3</b>
1.1.System Requirements.....	4
1.2.Sign up for Free ModSecurity Rules.....	4
1.3.Login to the Administration Console.....	9
1.4.The Administration Console - The Main Interface.....	11
<b>2. Deploy CWAF Rules On Server</b> .....	<b>13</b>
2.1.Linux - Install the Agent and Control Panel Plugin.....	13
2.2.Linux - Install the Agent in Standalone Mode .....	16
2.3.Windows - Install the Ruleset on Windows IIS .....	17
2.4.Use the Web Hosting Control Panel Plugin for Firewall Configuration.....	18
2.4.1.View and Update CWAF Information.....	20
2.4.2.Configure CWAF Parameters.....	23
2.4.3.Manage Security Engine.....	25
2.4.4.Configure Userdata.....	28
2.4.5.Send Feedback.....	29
2.4.6.Manage Catalog.....	30
2.4.7.Protection Wizard.....	32
2.5.Use the Agent for Firewall Configuration.....	36
2.6.Command Line Utility.....	36
2.7.Uninstall CWAF .....	38
2.8.Download and Install Rule Set Packages.....	39
2.9.Report Problems to Comodo.....	40
2.10.Submit Tickets to Comodo.....	41
<b>3. Managing CWAF License</b> .....	<b>41</b>
<b>4. CVE Coverage Information</b> .....	<b>43</b>
<b>Appendix 1 - Identifying Rule IDs for Exclusion</b> .....	<b>45</b>
<b>About Comodo Security Solutions</b> .....	<b>47</b>

# 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 Microsoft IIS, Apache, LiteSpeed and Nginx 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 'Linux - Installing The Agent And Control Panel Plugin' and 'Windows - Install The Ruleset On Windows IIS' 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 '**Linux - Installing The Agent And Control Panel Plugin**', '**Windows - Install The Ruleset On Windows IIS**' 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 Microsoft IIS web server, and Apache, LiteSpeed, 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

- **Linux - Installing the Agent and Control Panel Plugin** - Guidance on downloading and deploying the firewall rule sets on Linux
  - **Linux - Installing the Agent in Standalone Mode**
- **Windows - Install the Ruleset on Windows IIS** - Guidance on downloading and deploying the firewall rule sets on Windows
- **Using the Web Hosting Control Panel Plugin for Firewall Configuration** - Guidance on configuring firewall, rules and update the rule sets
- **Using the Agent for Firewall Configuration** - Guidance on manually downloading and deploying the latest version of the Firewall rulesets
- **Command Line Utility** - The list of arguments for protection rule management
- **Uninstalling CWAF** - Guidance on uninstalling CWAF on the web hosting control panel plugin
- **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 Tickets to Comodo** - Guidance on submitting support tickets to Comodo
- **Managing CWAF License** - Guidance on viewing and managing licenses and subscribing for other Comodo products and services
- **CVE Coverage Information** - Guidance on viewing on Common Vulnerabilities and Exposures.

## 1.1. System Requirements

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

- Microsoft IIS web server
- Apache, LiteSpeed or Nginx web server on Linux server platform
- Mod\_security 2.7.5 and higher

## 1.2. Sign 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.

**COMODO**  
Creating Trust Online®

## Comodo Web Application Firewall

1 Signup Information > 2 Confirmation > 3 Order Summary

### Comodo Sign-Up Page

Please, select currency that will be used for purchase (note that not all products can be available in currencies other than US Dollar)

US Dollar

Please, select product from the list

COMODO Web Application Firewall - No Card Required!

### Customer Information (an \* indicates required fields)

When you use credit card, the billing information should be exactly as it appears on your credit card statement. For credit card verification,

CWAF is available for free.

- Enter the customer information

### 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\***   
*Email is case-sensitive*

**Password\***   
(8 characters min.)  
*Password is case-sensitive*

**Password Confirmation\***   
*Password is case-sensitive*

**First Name\***

**Last Name\***

**Telephone Number\***

#### Contact Information

**Company Name\***

**Company Website**

**Street Address\***

**Address2**

**City\***

**Country\***

**State or Province**

**Postal Code\***

#### User Details:

- If you are a new to customer, select 'No' for 'Are you an existing Comodo customer?' and enter the in the appropriate fields. The fields marked with \* are mandatory.
- If you already have an account at Comodo Accounts Manager created while subscribing for some other product or you are renewing the CWF 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\***

Email is case-sensitive

**Login\***

(4 character min.)

Login is case-sensitive

**Password\***

(8 characters min.)

Password is case-sensitive

**Password Confirmation\***

Password is case-sensitive

### 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.

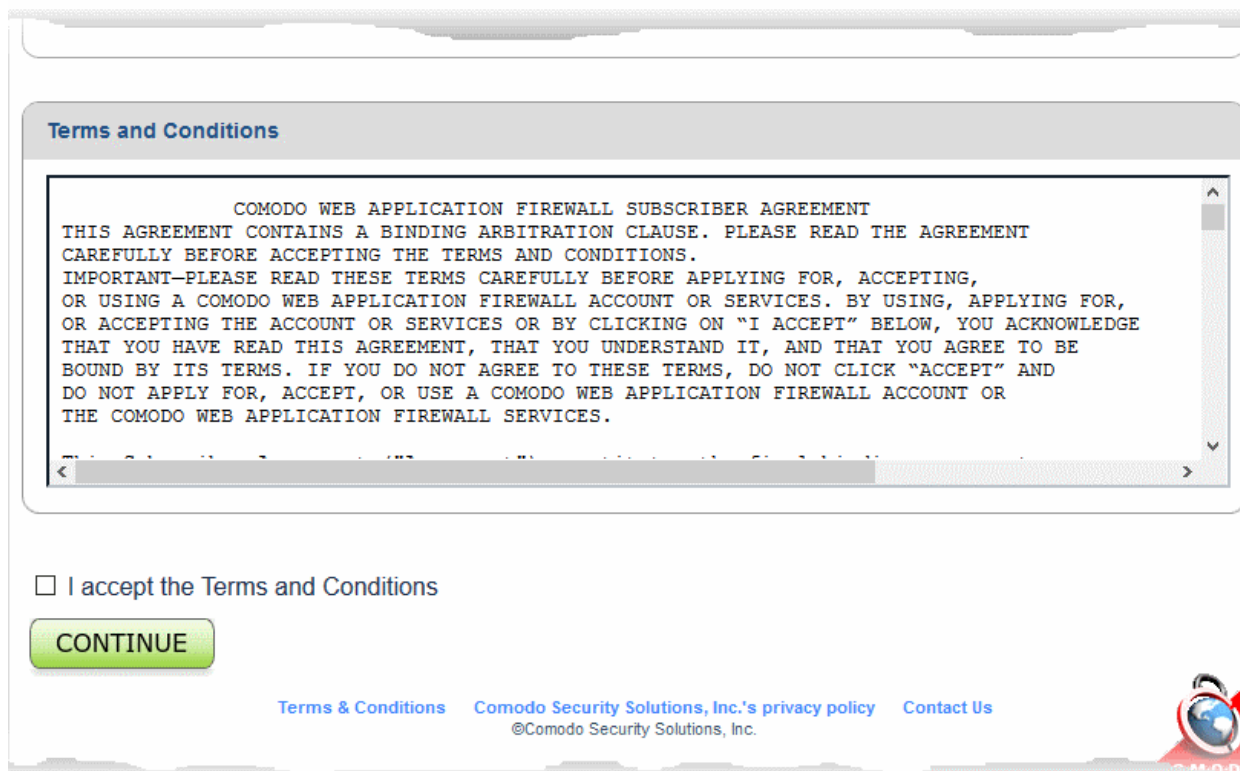
Postal Code

### Communication Options

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

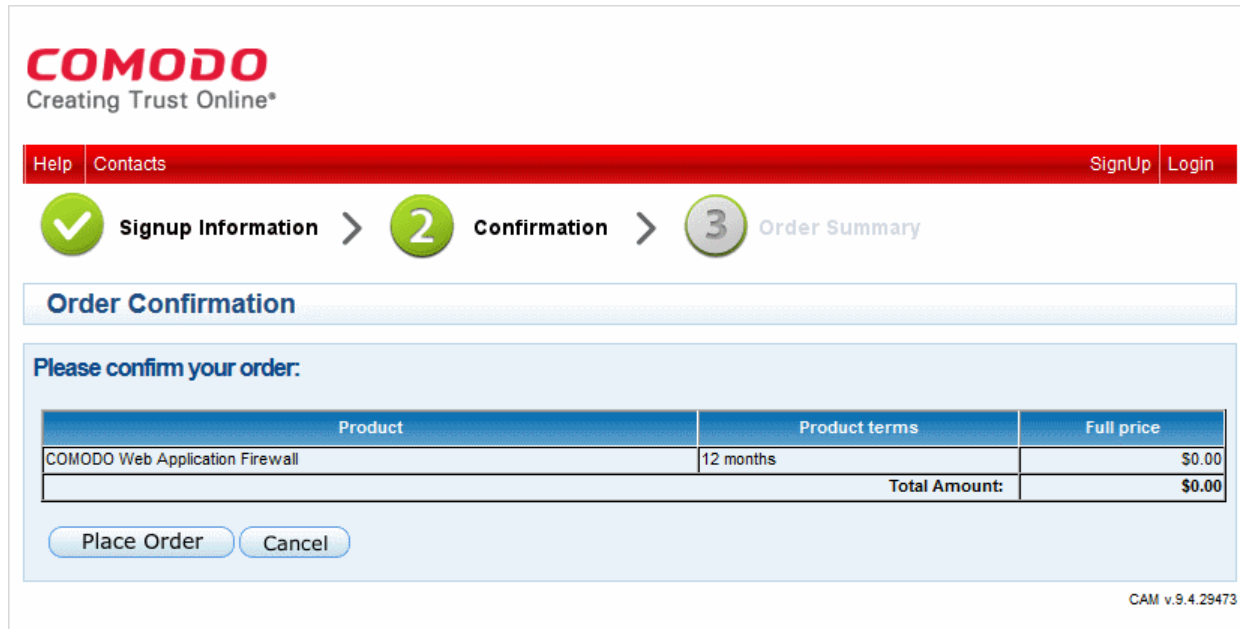
### Terms and Conditions:

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



- Click 'Continue'

The Order Confirmation page will appear.



- Click 'Place Order'

Your Order Summary will be displayed. Copy and paste your license key in a safe location.



Services
My Account
Help
Contacts
Logout

✓ Signup Information > 
 ✓ Confirmation > 
 3 Order Summary

Order #18929602-4

Comodo Security Solutions, Inc.  
1255 Broad Street  
Clifton, NJ 07013  
United States  
[support.comodo.com](mailto:support.comodo.com)

Account Information  
Billing  
Products  
Comodo WebApp  
FW

Thank you for your purchase. Your order is complete and the confirmation will be sent to your email shortly.

Subscription Details			
Product Name	License Key		
COMODO Web Application Firewall	868225e9-6c53-48a3-a7d5-ea933271dc3f		
INVOICE NUMBER	18929602-13	SUBSCRIPTION ID	bdc5312898

Order Details	
ORDER NUMBER	18929602-4
ORDER DATE	September 21, 2016
ORDER TOTAL	\$0.00
SUBSCRIPTION EXPIRES ON	September 21, 2017

How to get started: We will send you an email explaining how to download and install your Comodo Software. You will be asked to enter your License Key during the installation process.

You can access your Comodo Account via <https://accounts.comodo.com/account/login>. This login provides you with the ability to modify you password, add subscriptions for other products, change billing and contact information, and review the ongoing status of your service.

You will also receive an email containing your subscription ID, license key and instructions on downloading and installing the CWF agent on your server.

**Further Reading:**

- [Logging-in to the Administration Console](#)
- [Deploying CWF rules on Server](#)

## 1.3. Login to the Administration Console

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



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

You will be taken to the CWAF web administration console.

The screenshot shows the 'Version Management' page of the Comodo Web Application Firewall. At the top, it says 'Web Application Firewall POWERED BY COMODO'. There are three tabs: 'Ruleset version' (selected), 'License info', and 'CVE info'. A 'Welcome' message and a 'Logout' link are in the top right. Below the tabs, there's a 'Version Management' heading and a 'Latest release: 1.94' link. A blue bar contains filters for 'Source: Apache', 'Release: 1.x', and 'Version: 1.94', along with buttons for 'Download full ruleset', 'Download only updates', 'Report a problem with this version', and 'Submit Ticket to support'. The main content area is titled 'List of rule files' and shows 'Selected version: 1.94 (2016-09-13 14:53:31)'. A 'Short description' box lists CVEs and updates. Below is a table of rule files:

File Name	Status
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

## 1.4. The Administration Console - The Main Interface

Comodo Web Application Firewall (WAF) 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 administrators to download pre-defined rule-sets and to deploy them on their web application servers. Linux users can also download and install an agent that will automatically download and implement the rule-sets and update them when required. The agent can also install WAF plugins for popular control panels (cPanel, Plesk, DirectAdmin and Webmin) which allow administrators to configure rules and updates.

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 WAF agent from this interface.

The screenshot shows the 'Version Management' section of the Comodo WAF admin interface. It includes a navigation bar with tabs for 'Ruleset version', 'License info', and 'CVE CVE info'. Below the navigation bar, there are several callouts:

- Top Left:** 'The administrators can select the web sever, version of the Rule Set to be downloaded' (pointing to the 'Source' dropdown).
- Top Center:** 'The administrator can select whether to download the full Rule Set or only the updates from the previous version, of the selected version' (pointing to the 'Release' and 'Version' dropdowns).
- Top Right:** 'The administrator can submit feedback on the selected version by clicking this tab' (pointing to the 'Report a problem' button).
- Top Right (continued):** 'The administrator can download the latest version of the Rule Set, the agent set-up file or the help guide' (pointing to the 'Download full ruleset' and 'Download only updates' buttons).
- Bottom Right:** 'The administrator can submit a ticket to Comodo support' (pointing to the 'Submit Ticket to support' button).
- Center:** 'Displays the pre-defined Firewall Rule Sets in the selected version' (pointing to the 'List of rule files' table).

The 'List of rule files' table shows the following files and their status:

File Name	Status
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
08_Global_Other.conf	modified
09_Bruteforce_Bruteforce.conf	unmodified
10_HTTP_HTTP.conf	unmodified
11_HTTP_HTTPDoS.conf	unmodified
12_HTTP_Protocol.conf	modified

- **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 WAF 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.

The screenshot shows the 'Active license' page in the Comodo Web Application Firewall Admin Console. At the top, there is a navigation bar with three tabs: 'Ruleset version', 'License info' (which is selected), and 'CVE info'. Below the navigation bar, the page title is 'Active license'. Underneath, there is a section for 'License info' containing the following details: License: [redacted], License type: free, Product name: COMODO Web Application Firewall, and License expired at: 2016-07-22 04:35 UTC. A link to 'Manage your CAM account' is provided. At the bottom of the page, there is a footer with the text: 'Comodo Group, Inc. 2015. All rights reserved. All trademarks displayed on this web site are the exclusive property of the respective holders.'

## 2. Deploy CWF Rules On Server

Comodo Web Application Firewall allows or denies access to the web application based on firewall rule sets. Rule sets are made up from one or more individual firewall rules, each of which contains instructions that determine whether the application is allowed access; 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 which can be downloaded from the CWF console. Linux administrators can also ensure the latest rules are automatically implemented by installing the CWF Agent.

The agent can be configured to:

- Periodically poll the CWF server and to automatically download and install the latest firewall rule sets
- Install a web host control panel plugin to configure CWF

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

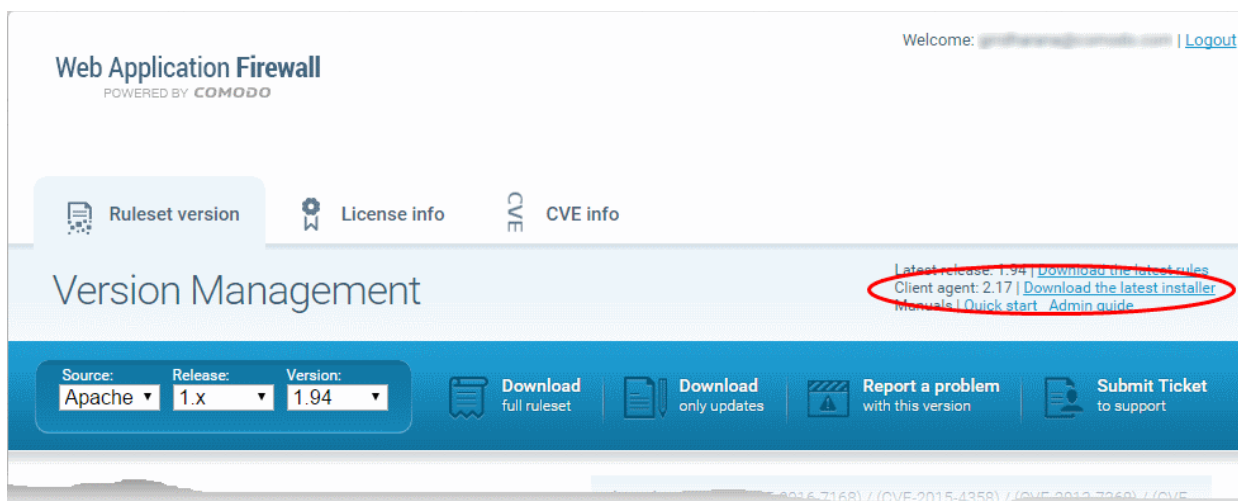
- [Linux - Install the Agent and Control Panel Plugin](#)
- [Windows - Install the Ruleset on Windows IIS](#)
- [Download and install Ruleset package](#)

### 2.1. Linux - Install the Agent and Control Panel Plugin

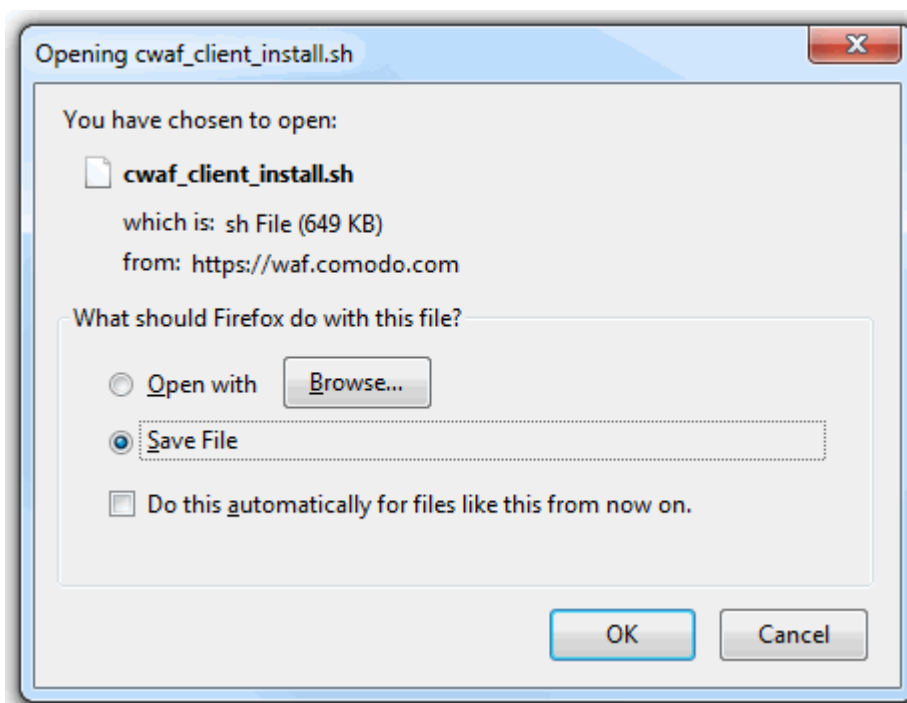
The CWF agent is a small piece of software that can be installed on your web server to automate the deployment of firewall rule sets and to configure CWF.

**To download the CWF agent installation file**

- Log-in to the web administration console at <https://waf.comodo.com>
- Ensure that the 'Ruleset version' tab is open
- Click the 'Download latest installer' link at the top right



The download dialog will appear.



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

The installer checks for web server type (Apache, LiteSpeed or Nginx) and any for installed control panels (cPanel, Plesk, DirectAdmin, Webmin).

### To install the web hosting control panel on to Linux 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 CWF 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"*:

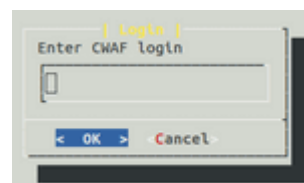
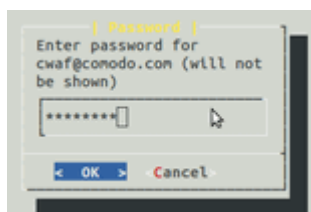
## Step 2

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



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 CWF and using the plug-in, refer to the section [Using Web Hosting Control Panel plugin for Firewall Configuration](#).

## 2.2.Linux - Install the Agent in Standalone Mode

### 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 on Linux](#) for more details.

### Step 4

#### Required for installation in standalone mode

Modify Apache Web Server configuration to enable 'mod\_security' module and include CWF Rules, by adding the key `'Include <CWF_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 CWF using the agent, refer to the section [Using the Agent for Firewall Configuration](#).



## 2.3. Windows - Install the Ruleset on Windows IIS

Please ensure you are running the following:

- IIS v 7.5.
- Mod\_security v 2.7.5 and above

### To install Mod-Security

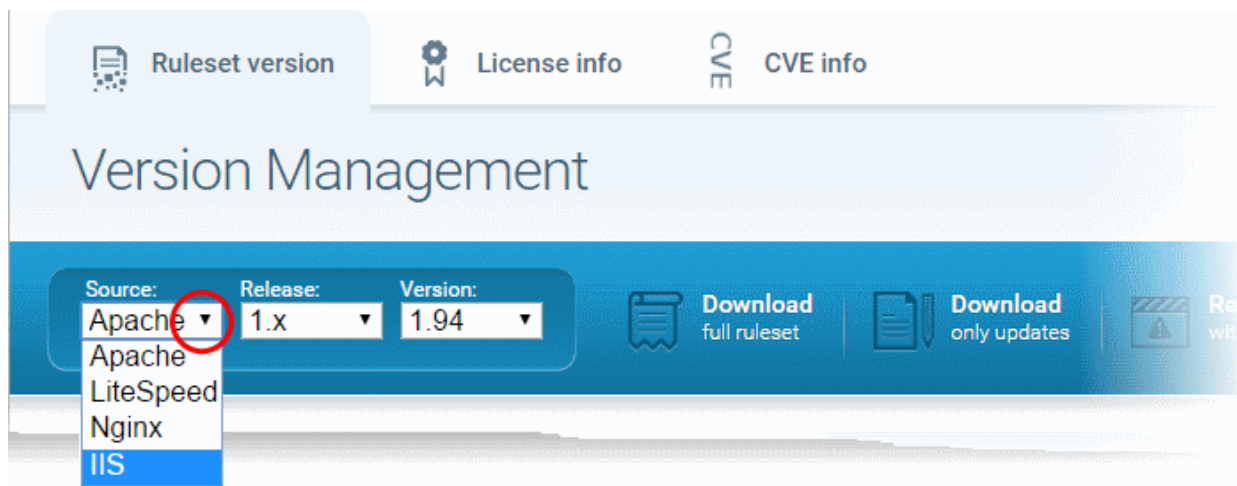
- Download and run the **Mod\_security installer**

Mod\_security can be included in any website by adding the following line to the web.config file, in system.webServer section:

```
<ModSecurity enabled="true" configFile="c:\path\to\cwaf\modsecurity_iis.conf" />
```

### To download and install CWAF rules

- Log-in to the web administration console at <https://waf.comodo.com/>
- Ensure that the 'Rule set version' tab is opened
- Select 'IIS' from the 'Source' 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.

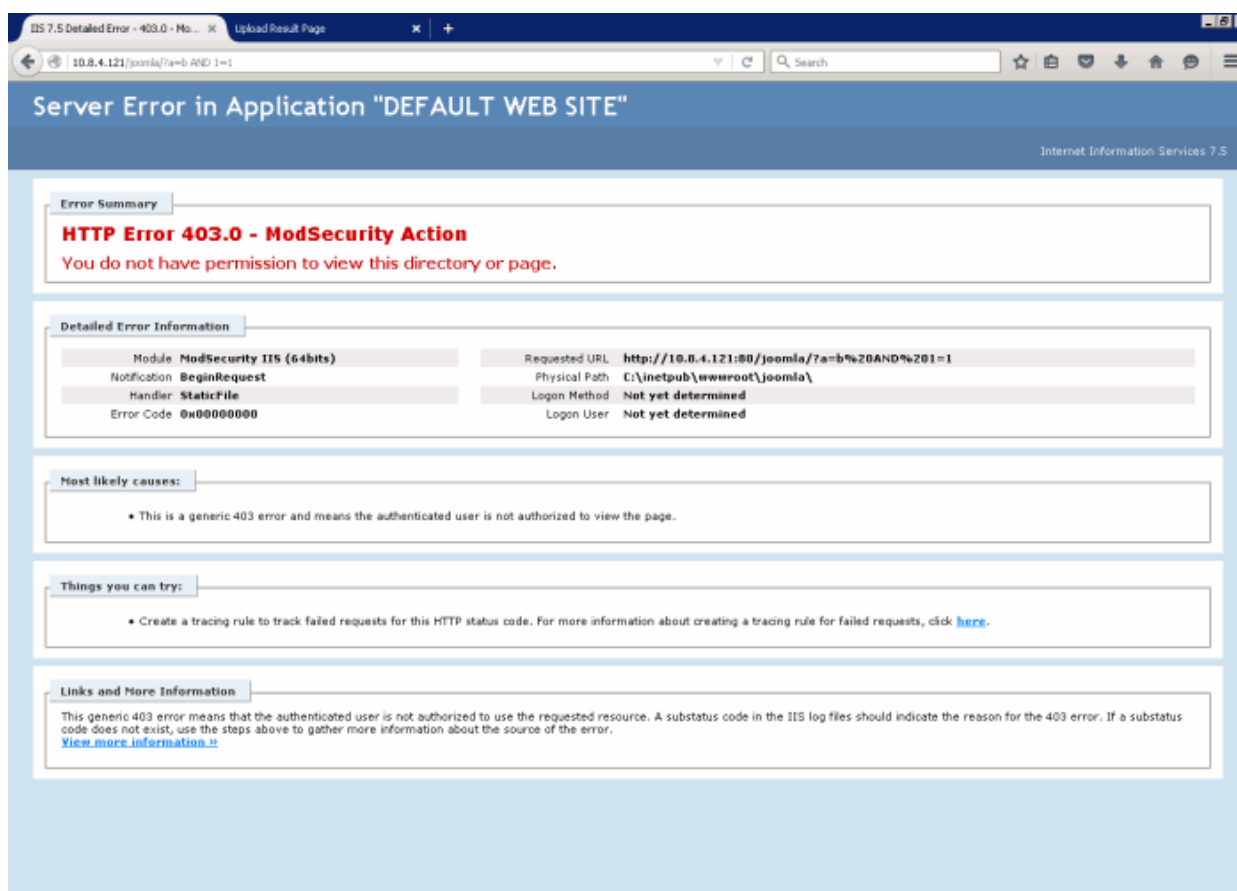


- Click 'Download full ruleset'
- Navigate to "C:\Program Files\ModSecurity IIS" and save the .zip file.
- Extract to "C:\Program Files\".
- Restart IIS.

To check CWAF for protection, send the request as shown below,

*http://your.server/?a=b AND 1=1*

The following warning will be displayed:



To run the protection rules updates,

- Go to the Start > Run > cmd.exe to open a command prompt
- Run system command:  
*cscript.exe "C:\Program Files\ModSecurity IIS\cwaf\_update.vbs"*

## 2.4. Use 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 CWF Webmin plugin

- Login to Webmin on your server
- Click on 'Servers' > '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	cWATCH
Current rules version	0						Rules 1.144 is available
CWAF plugin version	2.18 (Latest version)						
Web Platform	Apache						
Apache version	2.4.18						
Mod_security compatible	yes						
Mod_security loaded	yes						
Mod_security conf	/usr/local/apache/conf/modsec2.conf						
Found websites	8						

The interface has eight tabs:

- **Main** - Displays the versions of the currently loaded rule set, Apache server, Mod-Security status and number of **websites protected**. See '**Viewing CWAF Information**' for more details
- **Configuration** - Enables the administrator to view and edit CWAF configuration parameters. See '**Configuring CWAF Parameters**' for more details
- **Security Engine** - Enables the administrator to set up rules for Mod\_security option. See '**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. See '**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. See '**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. See '**Protection Wizard**' for more details.
- **cWatch** - Allows administrators to subscribe for and configure Comodo cWatch Web Security service for their servers. See the online help page <https://help.comodo.com/topic-285-1-785-10074-Configuring-cWatch-Web-Security.html> for more details.

## 2.4.1. View and Update 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

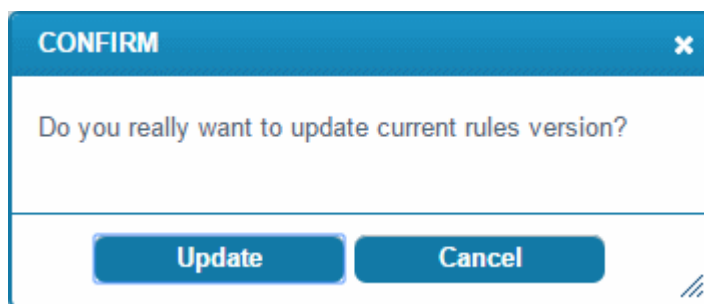
Main	Configuration	Security Engine	Userdata	Feedback	Catalog	Protection Wizard	cWATCH
Current rules version	0	<b>Rules 1.144 is available</b>					
CWAF plugin version	2.18 (Latest version)						
Web Platform	Apache						
Apache version	2.4.18						
Mod_security compatible	yes						
Mod_security loaded	yes						
Mod_security conf	/usr/local/apache/conf/modsec2.conf						
Found websites	8						

- **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

A confirmation message will be displayed.

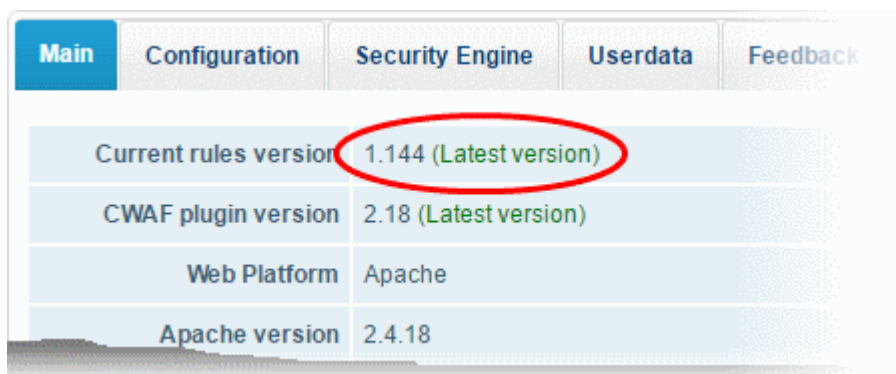


- Click 'Update'.

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



Wait till the page will be reloaded and the latest rule set will be available.



### To update the CWAF plugin to the latest version

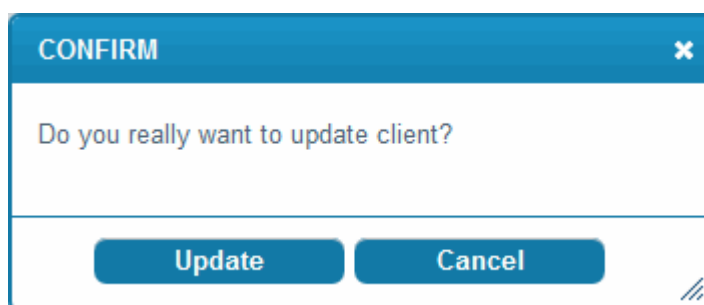
- Login to cPanel on your server
- Click 'Plugins' > "Comodo WAF"

- Click the 'Client X.X is available' at the far right side of the interface

## Web Application Firewall | Free ModSecurity Rules from Comodo

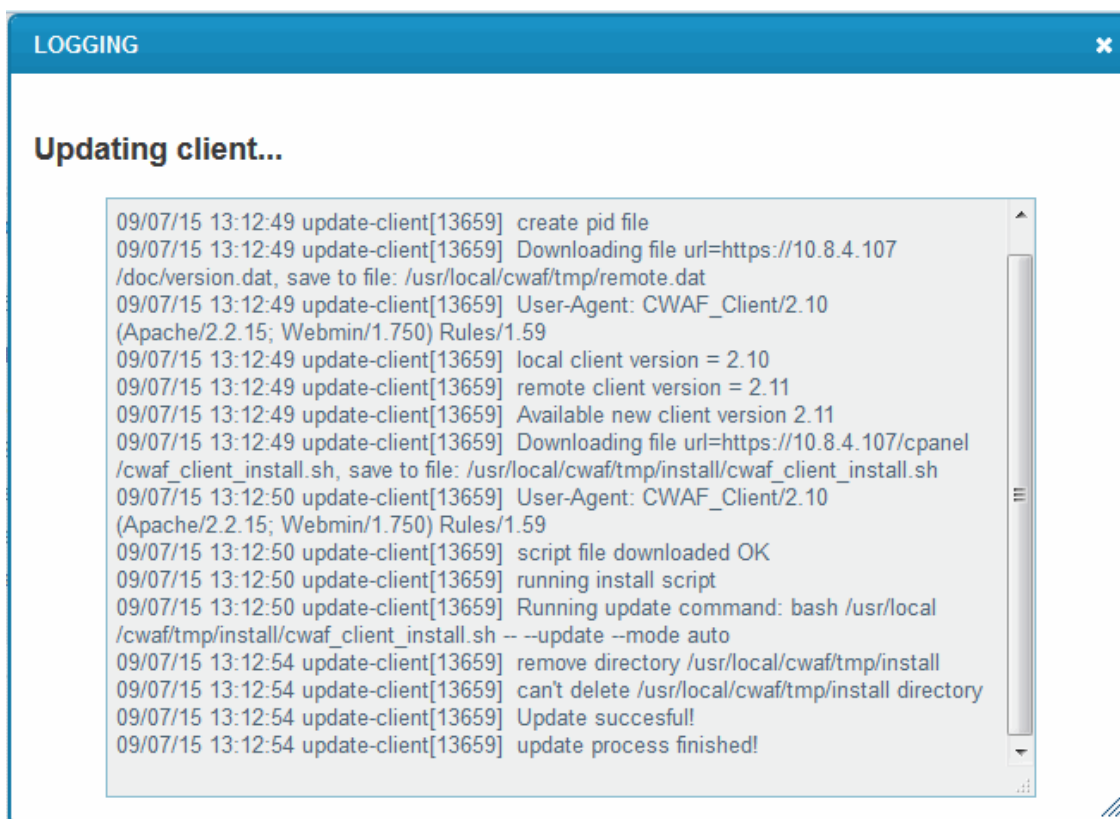


The confirmation message will be displayed.



Click 'Update'.

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

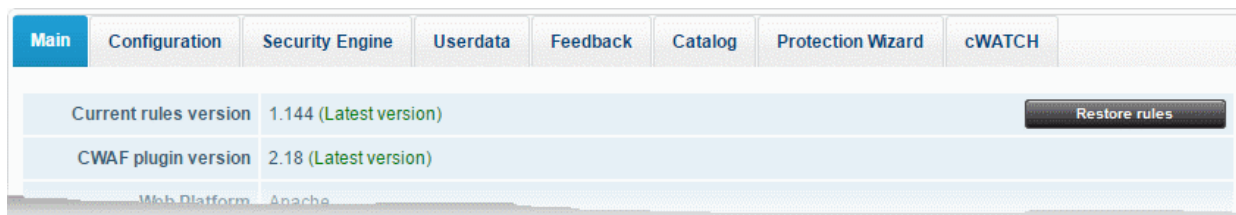


Wait till the page will be reloaded and the last plug-in version will be available.

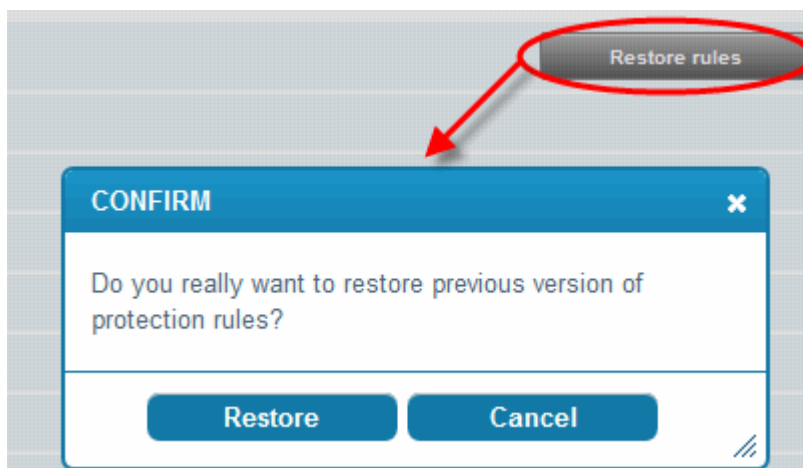
### To restore the rule set to the previous version

- Login to cPanel on your server

- Click 'Plugins' > "Comodo WAF"
- Click the 'Restore rules' at the far right side of the interface



The confirmation message will be displayed.



- 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/utills.log*

## 2.4.2. Configure CWAF Parameters

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

Main
Configuration
Security Engine
Userdata
Feedback
Catalog
Protection Wizard
cWATCH

### CWAF main configuration

Debug level:	<input style="width: 100%;" type="range"/> <div style="border: 1px solid #ccc; padding: 2px; margin-top: 2px;">1 (Critical)</div>
Log directory path:	<input style="width: 100%;" type="text" value="/var/log/CWAF"/>
Debug log:	<input style="width: 100%;" type="text" value="utils.log"/>
Consider subdomains:	<input checked="" type="checkbox"/>
Configuration backup:	<a href="#" style="background-color: #333; color: white; padding: 2px 10px; text-decoration: none;">Backup configuration</a>

### CWAF credentials

Comodo Login:	<input style="width: 100%;" type="text" value="cwaf@comodo.com"/>
Comodo Password:	<input style="width: 100%;" type="password"/>
Schedule Rules Update:	<div style="border: 1px solid #ccc; padding: 2px; display: inline-block;">Never ▼</div>

[Update config](#)

## 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.

- **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.

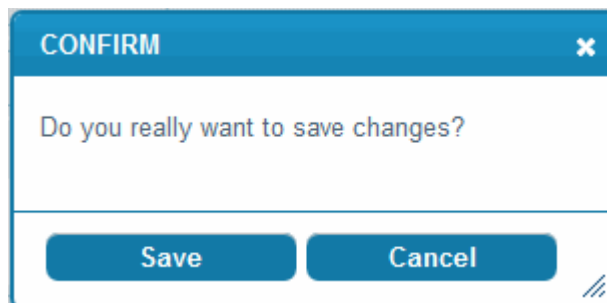
## CWAF credentials

- **Comodo Login** - The login user name for the CWAF account. This field is pre-populated with the username 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.



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

## 2.4.3. Manage 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.

Main	Configuration	Security Engine	Userdata	Feedback	Catalog	Protection Wizard	cWATCH
<b>Mod Security Configuration</b>							
Security Engine:	DetectionOnly ▾						<b>Disable domains</b>
Audit Engine:	Relevant Only ▾						
Set Server Signature:	<input checked="" type="checkbox"/>						
Audit Log:	/usr/local/apache/logs/modsec_audit.log						
Audit Log Storage:	/usr/local/apache/logs/modsec_audit						
Audit Log Type:	Serial ▾						
Debug log:	/usr/local/apache/logs/modsec_debug.log						
Debug Level:	<input type="text" value="0"/> 0 (None)						
Request Body Access:	On ▾						
Data Dir:	/tmp						
Temp Dir:	/tmp						
PCRE Match Limit:	250000						
PCRE Match Recursion:	250000						
<b>Update config</b>							

## 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**). Available 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 CWF events. (**Default:** **0**). The following table shows the list of levels:

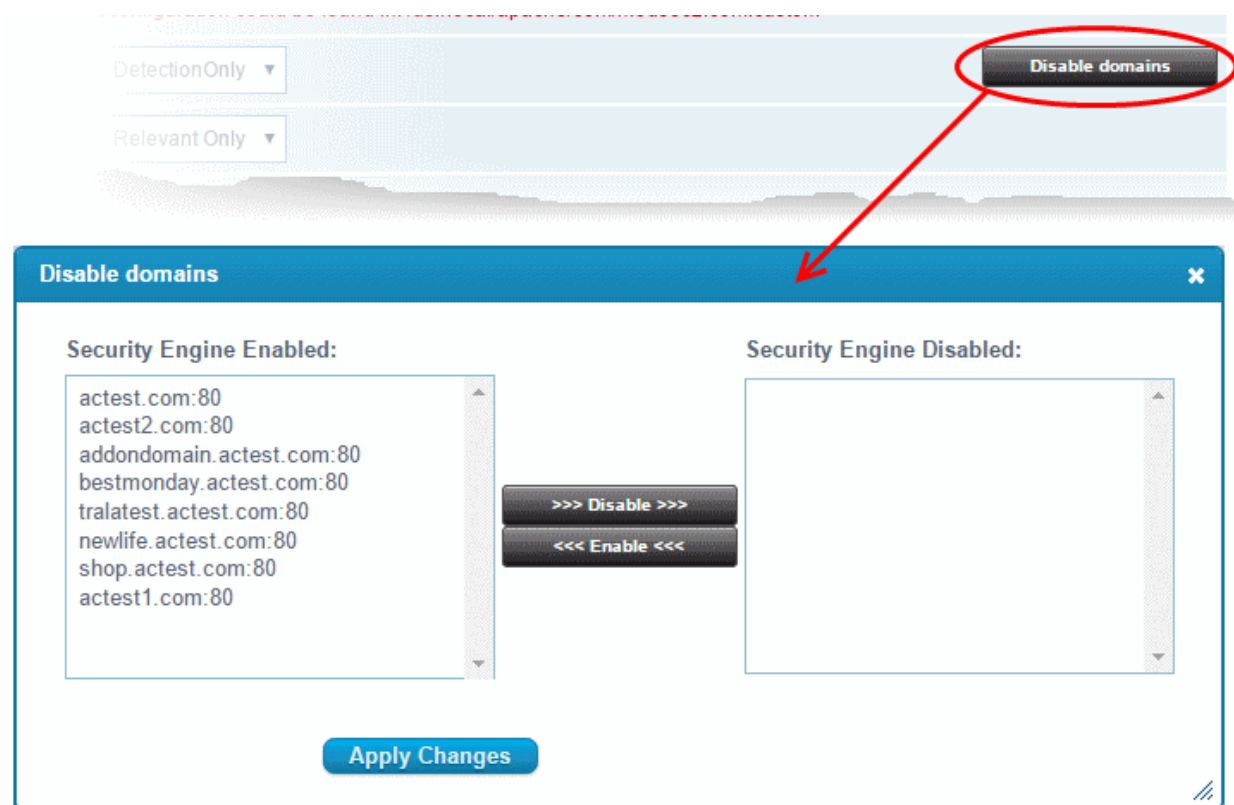
Level	Description
0	No events will be logged.
1	All errors (intercepted requests) will be logged.
2	All Warnings will be logged.
3	All Notifications will be logged.
4	Details of how transactions are handled will be logged.
5	As above but including information about each piece of information handled
6	
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:

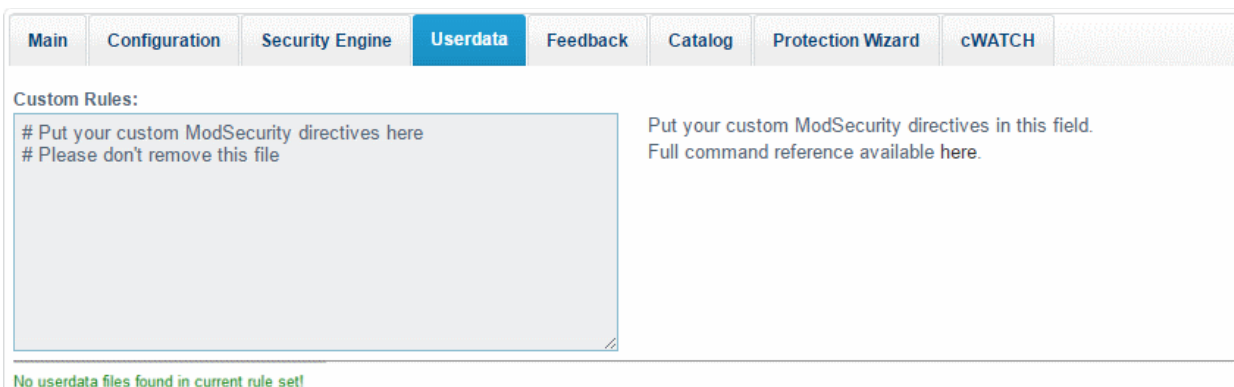


- Click on the domain or domains you wish to disable and click the '>>>Disable>>>' button to move it to the 'Disabled' list
- Click "Apply Changes" to save your configuration.
- Click 'Update Config' for your save your changes. The server will restart for your settings to take effect.

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

## 2.4.4. Configure Userdata

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



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

Main
Configuration
Security Engine
Userdata
Feedback
Catalog
Protection Wizard
cWATCH

**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 blocked then

---

**Blocked Extensions:**

```
# Put your extensions blacklist here
.asa/
.asax/
.ascx/
.axd/
.backup/
.bak/
.bat/
.cdx/
.cer/
...
```

Put file extensions which will be blocked (one extension per line).  
If you want to disallow serving of files with some extension you can add you restricted extensions here.

---

**Restricted Headers:**

```
# Put your headers blacklist here
/Proxy-Connection/
/Lock-Token/
/Content-Range/
/Translate/
/iff/
```

Put your restricted request headers here (one header per line).  
By default any request headers are allowed.  
If you want to block some request header then you should blacklist it here.

Save

## 2.4.5. Send 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.

Main Configuration Security Engine Userdata **Feedback** Catalog Protection Wizard cWATCH

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

Rules version: 1.144

Rule id(optional):

Type: rule gives false positive ▾

Message:

Send feedback

- **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.

## 2.4.6. Manage 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 CWF Information](#) for more details.

**Config:** Global config

Categories count: 9 Active categories: 6

**Content: categories list (global)** Filter by [Item ID]:  **Search By Rule ID**

Item ID	Description	Groups	Status	Excl
<a href="#">Apps</a>	Web Applications	7	<a href="#">ON</a>	
<a href="#">Bruteforce</a>	Bruteforce Protection	1	<a href="#">OFF</a>	
<a href="#">Global</a>	Global Protection	7	<a href="#">ON</a>	
<a href="#">HTTP</a>	HTTP-Related Protection	4	<a href="#">ON</a>	
<a href="#">Outgoing</a>	Preventing Information Reveal	8	<a href="#">OFF</a>	
<a href="#">PHP</a>	PHP Protection	1	<a href="#">ON</a>	
<a href="#">ROR</a>	Ruby On Rails protection	1	<a href="#">OFF</a>	
<a href="#">SQL</a>	SQL Protection	1	<a href="#">ON</a>	
<a href="#">XSS</a>	Cross Site Scripting	1	<a href="#">ON</a>	

- **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.
  - **Domains** - If you wish to apply actions to individual domains, click the arrow in the drop-down box and select the required domain.

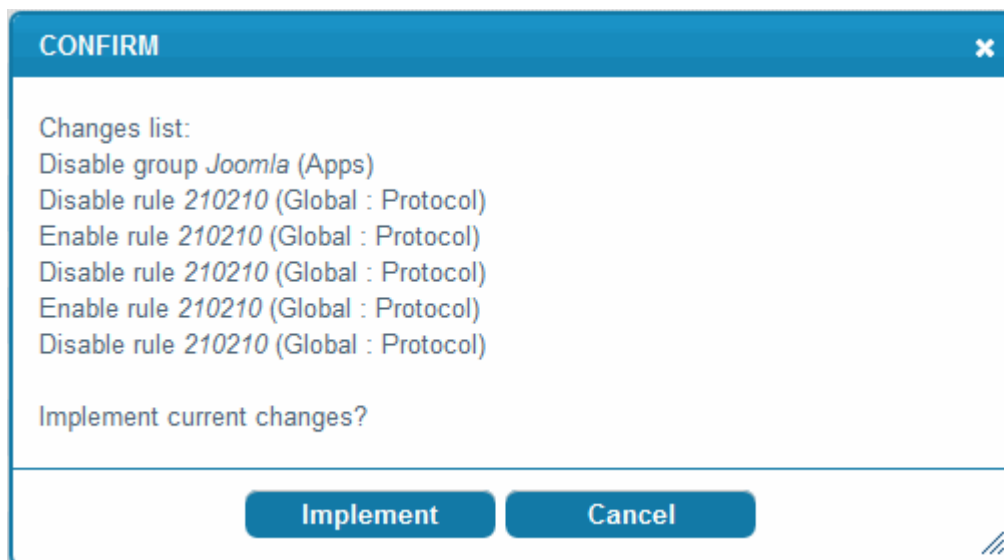
The catalog can be managed on three levels: categories, groups and rules. To navigate a level down link in 'Item ID' can be used.

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:



- Click 'Implement'.

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

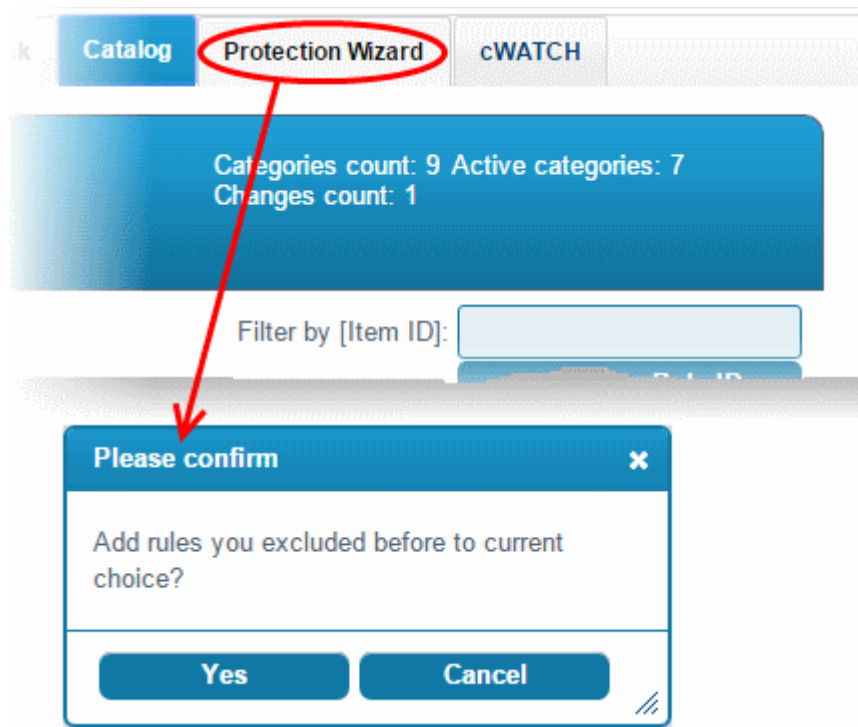
#### Filtering and search options:

- 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.

### 2.4.7. 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.





- 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.

<a href="#">Main</a>	<a href="#">Configuration</a>	<a href="#">Security Engine</a>	<a href="#">Userdata</a>	<a href="#">Feedback</a>	<a href="#">Catalog</a>	<b><a href="#">Protection Wizard</a></b>	<a href="#">cWATCH</a>
----------------------	-------------------------------	---------------------------------	--------------------------	--------------------------	-------------------------	--	------------------------

## 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.

**Next >**

By default, all categories are enabled.

- You can enable/disable categories as required.

Clicking the 'Next' button will display the 'Categories', 'Groups' and 'Rules' in a tree structure.

The screenshot shows the 'Protection Wizard' tab selected in the top navigation bar. Below the navigation bar is the 'Protection Tree' section with the instruction: 'Please check Categories/Groups/Rules you like to protect.' The tree contains the following items:

- +  SQL Protection
- +  Web Applications
- +  Cross Site Scripting
- +  PHP Protection
- +  HTTP-Related Protection
- +  Preventing Information Reveal
- +  Ruby On Rails protection
- +  Bruteforce Protection
- +  Global Protection

At the bottom of the tree are two buttons: '< Back' and 'Apply changes'.

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

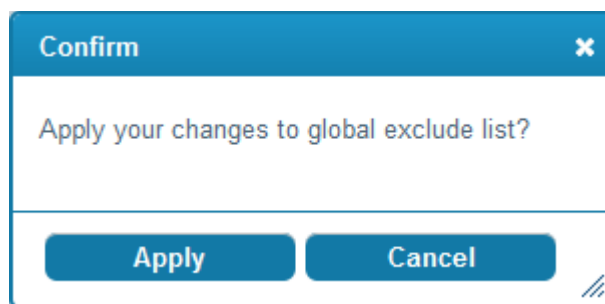
This screenshot shows the 'Protection Wizard' interface with the 'Web Applications' category expanded. The tree contains the following items:

- +  SQL Protection
- Web Applications
  - +  WordPress protection
  - +  WordPress Plugins protection
  - +  Joomla! components protection
  - +  WHMCS protection
  - +  Other apps protection
  - +  Joomla! protection
  - +  Drupal protection
- +  Cross Site Scripting
- +  PHP Protection
- +  HTTP-Related Protection
- +  Preventing Information Reveal
- +  Ruby On Rails protection
- +  Bruteforce Protection
- +  Global Protection

At the bottom of the tree are two buttons: '< Back' and 'Apply changes'.

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. A confirmation dialog will appear.



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

## 2.5. Use the Agent for Firewall Configuration

The agent allows Linux administrators 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/utills.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.

## 2.6. 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 CWF 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

## 2.7. Uninstall CWF

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 CWF 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 CWF 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 CWF 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 CWF 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.

## 2.8. Download and Install 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

Welcome: [admin@waf.comodo.com](#) | [Logout](#)

Web Application Firewall  
POWERED BY COMODO

Ruleset version License info CVE CVE info

Version Management

Latest release: 1.94 | [Download the latest rules](#)  
Client agent: 2.17 | [Download the latest installer](#)  
[Manuals](#) | [Quick start](#) | [Admin guide](#)

Source: Apache Release: 1.x Version: 1.94

Download full ruleset Download only updates Report a problem with this version Submit Ticket to support

List of rule files

Selected version: 1.94 (2016-09-13 14:53:31)

Short description: (CVE-2016-7168) / (CVE-2015-4358) / (CVE-2013-7368) / (CVE-2015-3922) / (CVE-2015-3921) / (CVE-2015-1052) / (CVE-2013-7349) / SSRF/XSPA Vulnerability in Dotclear 2.9.1 / XSS Vulnerability in the ClipBucket 8.2.1 / bl\_domains update

- If you want to download a selected version of the rule set,
  - Select the source from the 'Source' drop-down
  - 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 source version of the package will be listed under 'List of rule files', along with its release date and time.

Web Application Firewall  
POWERED BY COMODO

Welcome: [admin@comodo.com](#) | [Logout](#)

Ruleset version License info CVE CVE info

Version Management

Latest release: 1.94 | [Download the latest rules](#)  
Client agent: 2.17 | [Download the latest installer](#)  
Manuals | [Quick start](#) [Admin guide](#)

Source: Apache Release: 1.x Version: 1.94

Download full ruleset Download only updates Report a problem with this version Submit Ticket to support

List of rule files

Selected version: 1.94 (2016-09-13 14:53:31)

Short description: (CVE-2016-7168) / (CVE-2015-4358) / (CVE-2013-7368) / (CVE-2015-3922) / (CVE-2015-3921) / (CVE-2015-1052) / (CVE-2013-7349) / SSRF/XSPA Vulnerability in Dotclear 2.9.1 / XSS Vulnerability in the ClipBucket 8.2.1 / bl\_domains update

- 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'

Your download will start.

#### 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 CWF 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 CWF help guide, click the 'Manual' shortcut link at the top right.

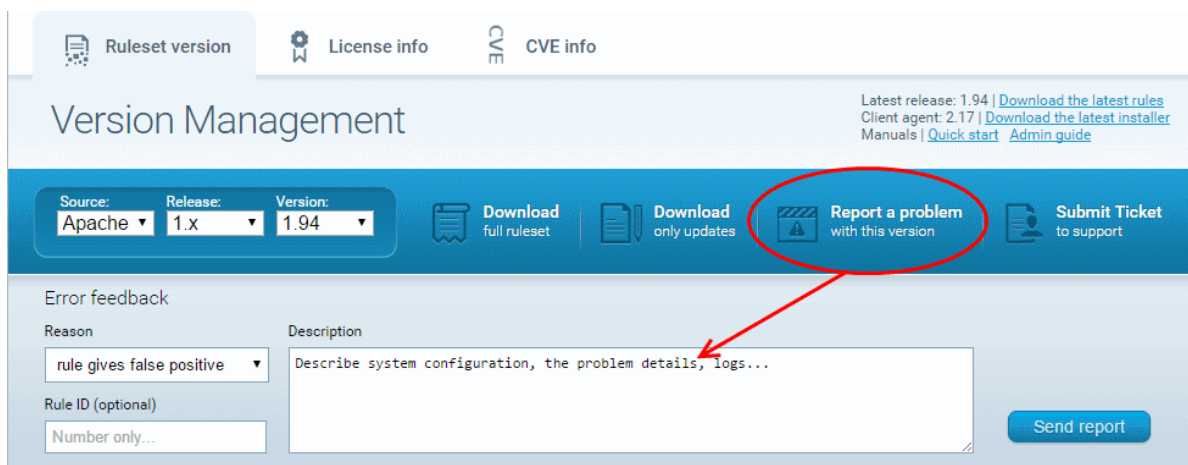
## 2.9. Report Problems to Comodo

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.

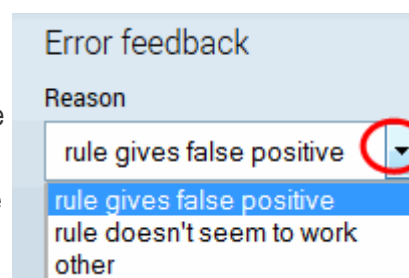
#### To submit feedback

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





- **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.



Click 'Send report' to submit to Comodo.

## 2.10. Submit 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 CWFAF 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.



Web Application Firewall  
POWERED BY COMODO

Welcome: cwaf@comodo.com | [Logout](#)

Ruleset version License info CVE CVE info

## Active license

### License info

**License:** `7d87e2c4-82e6-42e0-828b-ff5a10f25e7`  
**License type:** free  
**Product name:** COMODO Web Application Firewall  
**License expired at:** 2016-07-22 04:35 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.

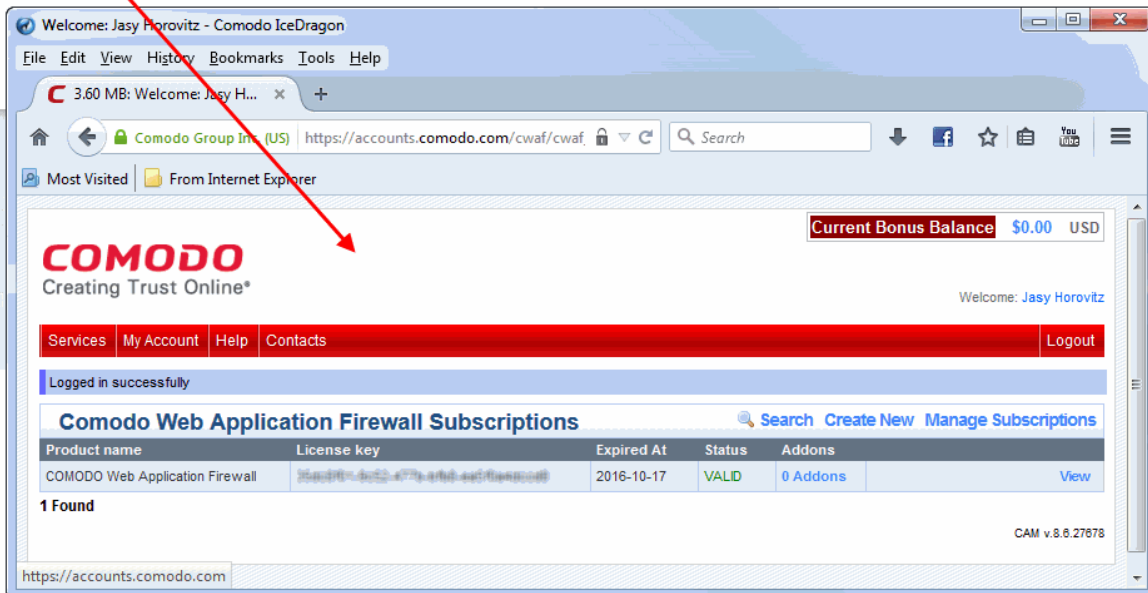
- **License** - Displays the account license key.
- **License type:** Displays the type of license - free or paid.
- **Product name** - Displays the name of the product for which you have a license.
- **License expired at** - Displays the expiration date of the license.
- **Manage your CAM account** - 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: :852be2c198b-4790-8849-6382cc09a6f6  
License type: free  
Product name: COMODO Web Application Firewall  
License expired at: 2016-05-19 13:53 UTC

[Manage your CAM account](#)



## 4. CVE Coverage Information

You can view without concealment information of a potential security vulnerabilities and exposure names to enhance capacity to remediate the problem.

The 'CVE info' interface consisting of two parts,

1. CVE information: CVE ID, CVE Creation and Update Date, CVE Description, CVE Related Links
2. CWAF information: whether or not CVE is covered by CWAF rules, CWAF rules that covered CVE and CWAF rules version that covers CVE

The screenshot displays the 'Web Application Firewall' admin console interface. At the top, it says 'Web Application Firewall POWERED BY COMODO'. The user is logged in as 'cwaf@comodo.com'. There are navigation tabs for 'Ruleset version', 'License info', and 'CVE CVE info'. The 'CVE CVE info' tab is active. Below the tabs is a search bar with the text 'Search for CVE'. The search input field contains 'CVE-2013-0235' and a dropdown menu is set to 'Search for CVE'. A blue 'Search' button is to the right. The search results show details for CVE ID CVE-2013-0235, including its creation date (12/06/2012), update date (06/11/2015), and a description: 'The XMLRPC API in WordPress before 3.5.1 allows remote attackers to send HTTP requests to intranet servers, and conduct port-scanning attacks, by specifying a crafted source URL for a pingback, related to a Server-Side Request Forgery (SSRF) issue.' There are also several links provided. Below the description is a section titled 'Rules' which lists two rules: Rule ID: 240330 (Covered in version: 1.45) and Rule ID: 219000 (Covered in version: 1.45). At the bottom, there is a copyright notice: 'Comodo Group, Inc. 2015. All rights reserved. All trademarks displayed on this web site are the exclusive property of the respective holders.'

To access the CVE info,

- Log-in to the web administration console at <https://waf.comodo.com/>
- Open 'CVE Info'
- Select the CVE ID from the 'Search for CVE' drop-down then click 'Search'

The description for each vulnerability or exposure and dedicated WAF rules will be displayed.

# 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"
```

*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 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 : +1.888.266.636

Tel : +1.703.581.6361

<https://www.comodo.com>

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