COMODO
Creating Trust Online®

Web Application Firewall
POWERED BY COMODO

Comodo
Web Application Firewall

Software Version 2.11

Quick Start Guide

Guide Version 2.11.071315

Comodo Security Solutions
1255 Broad Street
Clifton, NJ 07013

1.Comodo Web Application Firewall - Quick Start Guide

This tutorial briefly explains how an administrator can setup and configure Comodo Web Application Firewall (CWAF) - the customizable rules based traffic control system that protects your web based applications.

This quick start guide will take you through the following processes - click on any link to go straight to that section as per your current requirements.

- **Step-1 - Sign-up for Comodo Web Application Firewall**
- **Step 2 - Login to admin console**
- **Step 3 - Download rule sets and deploy on to server by anyone of the following methods:**
    - **Using CWAF plugin for automatic download and deployment of rule sets**
    - **Using CWAF Agent to download and implement the rule sets**
    - **Downloading the rule sets from web admin console and installing on to server**

Step-1 - Signing-up for Comodo Web Application Firewall

- Sign-up for the CWAF service from the Comodo Accounts Manager at **https://accounts.comodo.com/cwaf/management/signup**.
- Select the CWAF product from the list
- Fill-in your user details and billing information
- Select the payment mode and enter your payment details
- Read the 'End User License and Subscriber Agreement' and accept to it by selecting 'I accept the Terms and Conditions' checkbox.
- Click 'SIGN UP'

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

Step 2 - Login to Admin 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.

Step 3 - Download rule sets and deploy on to server

Comodo periodically publishes pre-defined firewall rule sets for the CWAF, which can be downloaded and deployed on to your web application server. You can follow any one of the methods given below to download and deploy the rule sets, and to keep them up-to-date.

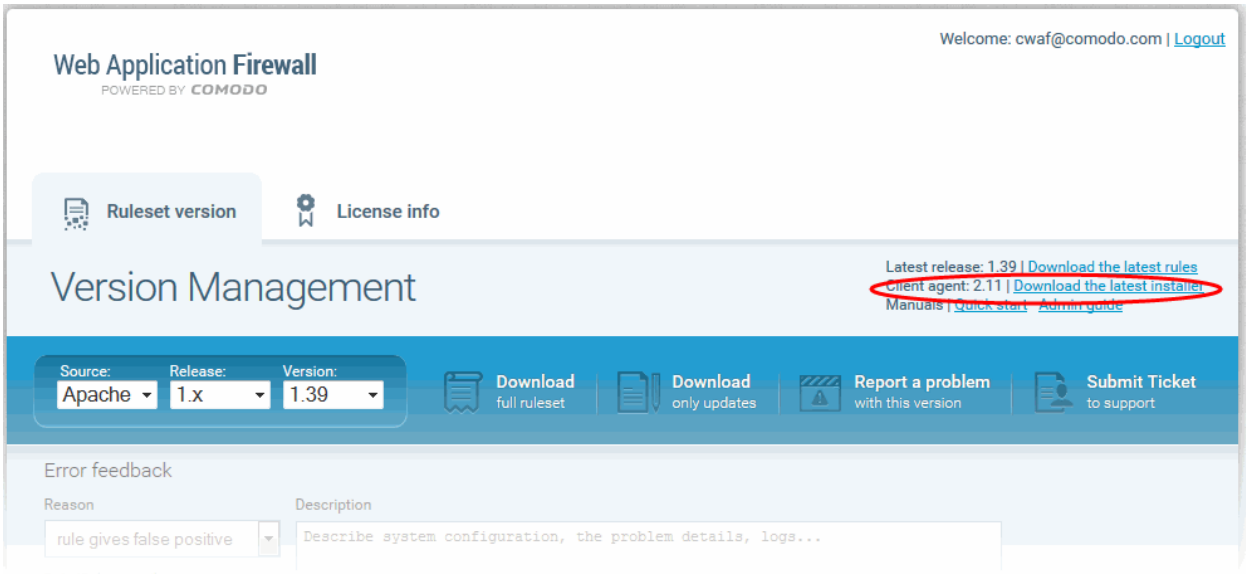
- **Using CWAF web hosting control panel plugin for automatic download and deployment of rule set updates**
- **Using CWAF Agent to download and implement the rule sets**
- **Downloading the rulesets from web admin and installing on to server**

Using plugin for automatic download and deployment of rule set updates

You can download the CWAF agent from the admin console and install on to the server to create a plugin that enables you configure the overall behavior of CWAF. The plugin can be used to automatically download the periodically updated rule sets and to deploy them on to your server.

Downloading the Agent

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



- Download and save the agent setup file

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 be 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*

Checking for mod_security and its version:

To ensure there are no syntax errors. If errors are found, a warning message will be displayed: *Apache config syntax should be correct 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 script 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

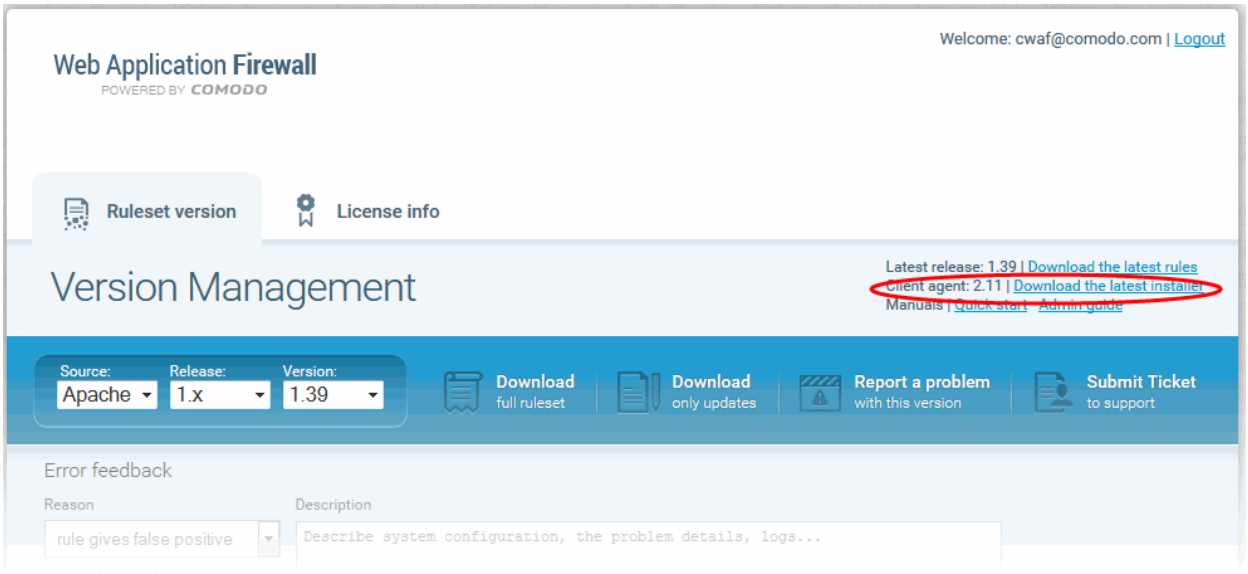
The agent will be installed on the server at */var/cpanel/cwaf* with a cPanel plugin or at */usr/local/cwaf* with a Plesk plug-in. For more details on configuring CWAF and using the plug-in, refer to the section **Using Web Hosting Control Panel plugin for Firewall Configuration.**

Using CWAF Agent to Download and Deploy the Rule Sets

You can download CWAF agent from the admin console and install on to the server to and use it to download and deploy the periodically published firewall rule sets.

Downloading the Agent

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



- Download and save the agent setup file

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

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"

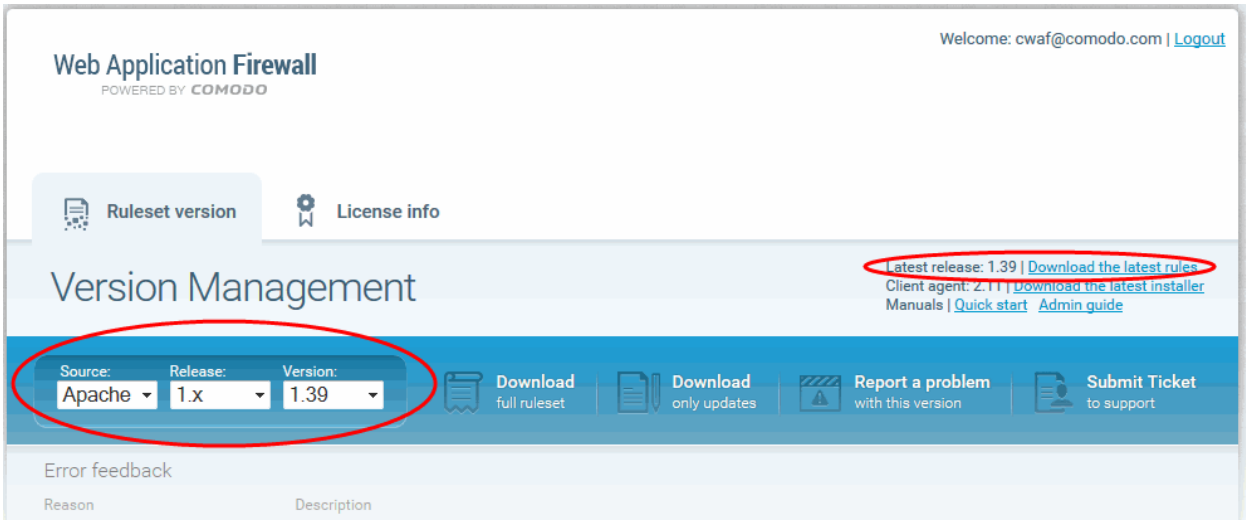
and reload Apache

After Installation is complete, please r*estart Apache server.*

The agent, in this example, is installed on the server at the path */opt/cwaf*. Refer to the online help page Refer to **Installing The Web Hosting Control Panel Plugin** section on using the agent for deploying the firewall rule sets.

Downloading the rule sets from web admin console and installing on to server

- Log-in to the web administration console at **https://waf.comodo.com** and ensure that the 'Rule set version' tab is opened.
- Click the 'Download latest rules set' shortcut link at the top right to download the latest version of the rules set package or choose a source and version from the 'Select version' drop-down and choose the release number from the 'Select release' drop-down to download the rules set package of a selected version.



- Download and save the rule set package file.
- 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.

Refer to the online help page **Downloading and installing rule set packages** of the **CWAF Admin Guide** for more details on using the web admin console.

To access the CWAF cPanel plugin

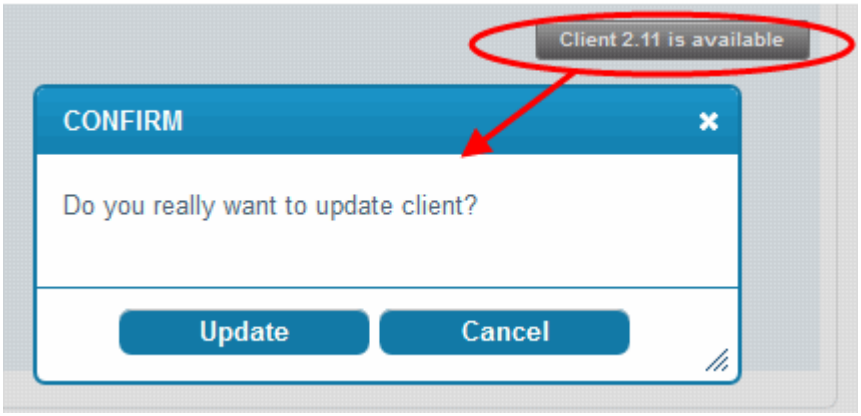
- Login to cPanel on your server
- Click 'Plugins' > "Comodo WAF".

The Comodo Web Application Firewall configuration screen will appear.

- Click on the 'Main' tab

The Main tab enables the administrator to manually update the currently loaded rule set to the latest version or to restore to the previous version.

- To update the rule set to the latest version, click 'Rules X.XX is available'



The updater will automatically download and deploy the latest version of rule set. You can view the update logs for the details on updates at:

/var/log/CWAF/utils.log

Refer to the online help page **Using The Web Hosting Control Panel Plugin For Firewall Configuration** of the **CWAF Admin Guide** for more details on configuring the web application firewall through the plugin interface.

To access the CWAF DirectAdmin plugin

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

The Comodo Web Application Firewall configuration screen will appear. The functionality and appearance of DirectAdmin Plugin is the same as for cPanel plugin. Refer to the online help page **Using The Web Hosting Control Panel Plugin For Firewall Configuration** of the **CWAF Admin Guide** for more details on configuring the web application firewall through the plugin interface.

To access the CWAF Plesk plugin

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

The Comodo Web Application Firewall configuration screen will appear. The functionality and appearance of Plesk Plugin is the same as for cPanel plugin. Refer to the online help page **Using The Web Hosting Control Panel Plugin For Firewall Configuration** of the **CWAF Admin Guide** for more details on configuring the web application firewall through the plugin interface.

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. The functionality and appearance of Webmin Plugin is the same as for cPanel plugin. Refer to the online help page Refer to **Using The Web Hosting Control Panel Plugin For Firewall Configuration** of the **CWAF Admin Guide** for more details on configuring the web application firewall through the plugin interface.

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.**