

Web Application Firewall
POWERED BY **COMODO**

Comodo

Web Application Firewall

Software Version 1.1

Administrator Guide

Guide Version 1.1.010614

Table of Contents

1.Comodo Web Application Firewall - Introduction.....	3
1.1.System Requirements.....	3
1.2.Signing up for Web Application Firewall.....	4
1.3.Logging-in to the Administration Console.....	8
1.4.The Administration Console - The Main Interface.....	10
2.Deploying CWAF rules on Server.....	12
2.1.Downloading and installing rule set packages.....	12
2.2.Using the CWAF Agent.....	14
2.2.1.Installing the agent for deploying the Rule Sets.....	15
2.2.2.Using the Agent for Firewall Configuration.....	16
2.2.3.Installing the Agent for cPanel Plug-in.....	16
2.2.4.Using the cPanel Plug-in for Firewall Configuration.....	17
2.2.5.Uninstalling the CWAF Agent.....	23
2.3.Reporting Problems to Comodo.....	23
3.Managing CWAF License.....	24
Appendix 1 - Identifying Rule IDs for Exclusion.....	27
About Comodo.....	28

1. Comodo Web Application Firewall - 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 and Linux based web-servers.

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. Alternatively, administrators can install the CWAF agent or the cPanel agent to automatically fetch and install the new rules as soon as they become available. The agents 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 on Linux servers. Versions for other web-server types are coming shortly.

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
 - **Downloading and installing rule set packages** - Guidance on manually downloading and deploying the firewall rule sets
 - **Using the CWAF Agent** - Guidance on using the CWAF agent for downloading and deploying the firewall rule sets
 - **Installing the agent for deploying the Rule Sets**
 - **Using the Agent for Firewall Configuration**
 - **Installing the Agent for cPanel Plug-in**
 - **Using cPanel Plug-in for Firewall Configuration**
 - **Uninstalling the CWAF Agent**
- **Reporting Problems to Comodo** - Guidance on posting feedback 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 web server on Linux server platform

1.2. Signing up for Web Application Firewall

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*	<input type="text" value="jsmith@example.com"/>
Password* (8 characters min.)	<input type="password" value="•••••"/>
Password Confirmation*	<input type="password" value="•••••"/>
First Name*	<input type="text" value="John"/>
Last Name*	<input type="text" value="Smith"/>
Telephone Number	<input type="text" value="12345678"/>

Contact Information

Company Name	<input type="text" value="J C Dithers Construction Cor"/>
Street Address*	<input type="text" value="ABC Street"/>
Address2	<input type="text" value="XYZ Area"/>
City*	<input type="text" value="City Name"/>
Country*	<input type="text" value="United States"/>
State or Province	<input type="text" value="Alabama"/>
Postal Code*	<input type="text" value="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 CWF license, select 'Yes' for 'Are you an existing Comodo customer?'. You will need to fill only your Login 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.)

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* ▼

State or Province ▼


Postal Code*





Payment Options

Payment Options:

The same as contact information. 

Payment Options

☐ 

☐    

☐ 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* -

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 ACKNOWLEDGE 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'

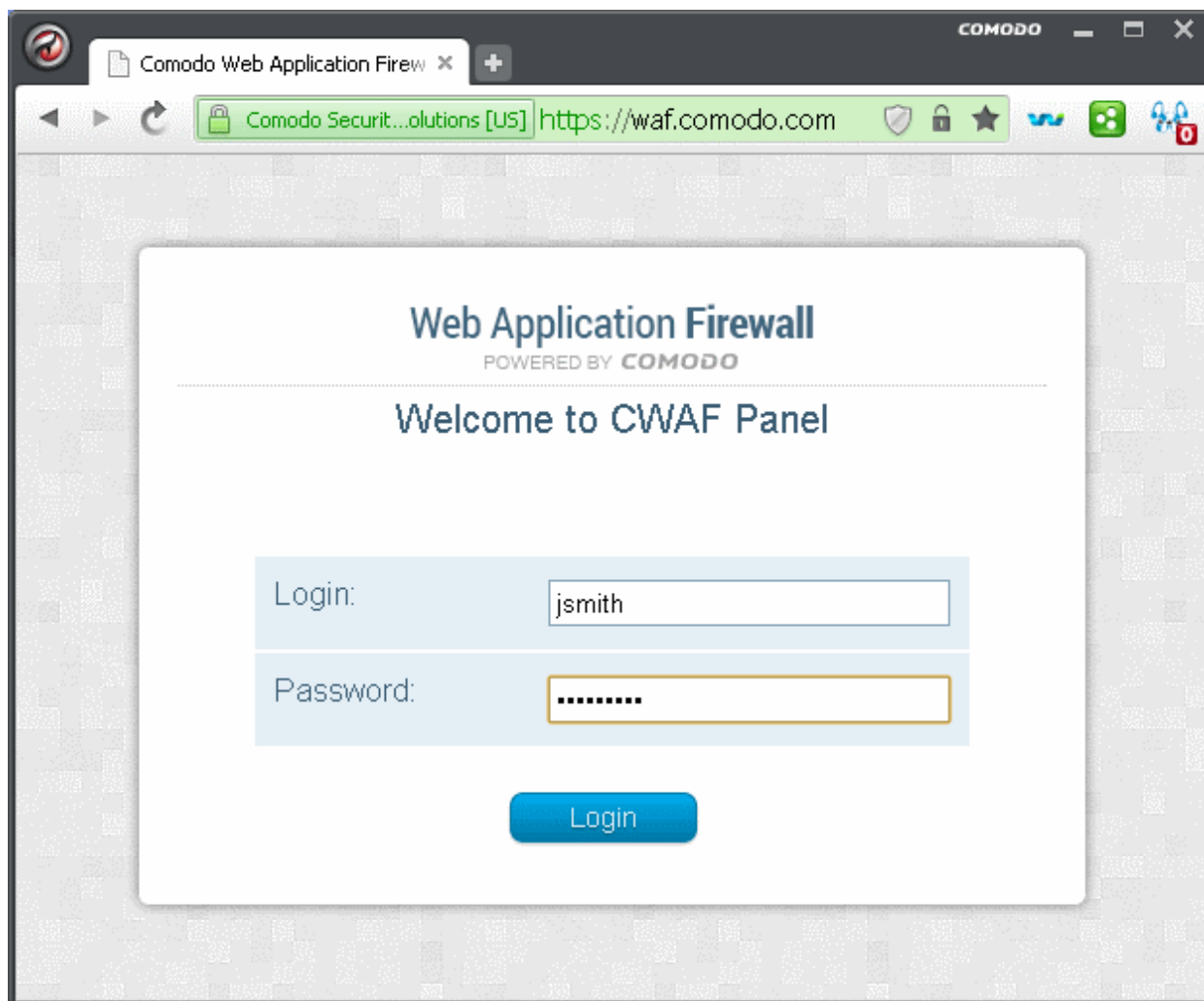
Upon successful payment processing, your account will be activated. You can sign-in to Comodo Web Application Firewall administration interface at <https://waf.comodo.com> with the same username and password you specified during signing up and manage your Web Application Firewall.

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>.



- 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 administration console. At the top, there's a header with the 'Web Application Firewall' logo and 'POWERED BY COMODO'. A user is logged in as 'jsmith' with a 'Logout' link. Below the header, there are two tabs: 'Rules set version' (active) and 'License info'. The main content area is titled 'Version Management'. On the right, it shows the 'Latest release: 0.10' with a link to 'Download latest rules set' and 'Client agent: 0.1' with a link to 'Download latest installer'. Below this, there's a blue bar with three buttons: 'Download full rules set', 'Download only updates', and 'Report a problem with this version'. The main section is titled 'List of rule files' and shows the 'Selected version: 0.10 (2013-07-29 13:53:51)'. A 'Short description' box indicates 'Removed 2 nasty rules'. A table lists rule files and their status:

File Name	Status
bl_domains	unmodified
bl_malwares	unmodified
bl_names	unmodified
bl_sql	unmodified
cwaf_01.conf	unmodified
cwaf_02.conf	unmodified
cwaf_03.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 rulesets 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 rulesets and which will update them whenever the rules are updated by Comodo. The agent also installs a cPanel plug-in that facilitates the configuration of updates. The Administrator can also view, renew or upgrade the WAF 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 WAF agent from this interface.

The screenshot shows the 'Web Application Firewall' admin interface. At the top, there's a 'Welcome: jsmith | Logout' link. Below the header, there are two tabs: 'Rules set version' and 'License info'. The 'Rules set version' tab is active, showing a 'Version Management' section. This section includes a 'Select release' dropdown (set to '0.x') and a 'Select version' dropdown (set to '0.10'). Below these are three buttons: 'Download full rules set', 'Download only updates', and 'Report a problem with this version'. To the right of these buttons, there's a link for 'Latest release: 0.10 | Download latest rules set' and another for 'Client agent: 0.1 | Download latest installer'. Below the buttons, there's a 'List of rule files' section. It shows a 'Selected version: 0.10 (2013-07-29 13:53:51)' and a 'Short description: Removed 2 nasty rules'. Below this, there's a table of rule files:

Rule File	Status
bl_domains	unmodified
bl_malwares	unmodified
bl_names	unmodified
bl_sql	unmodified
cwaf_01.conf	unmodified
cwaf_02.conf	unmodified
cwaf_03.conf	unmodified

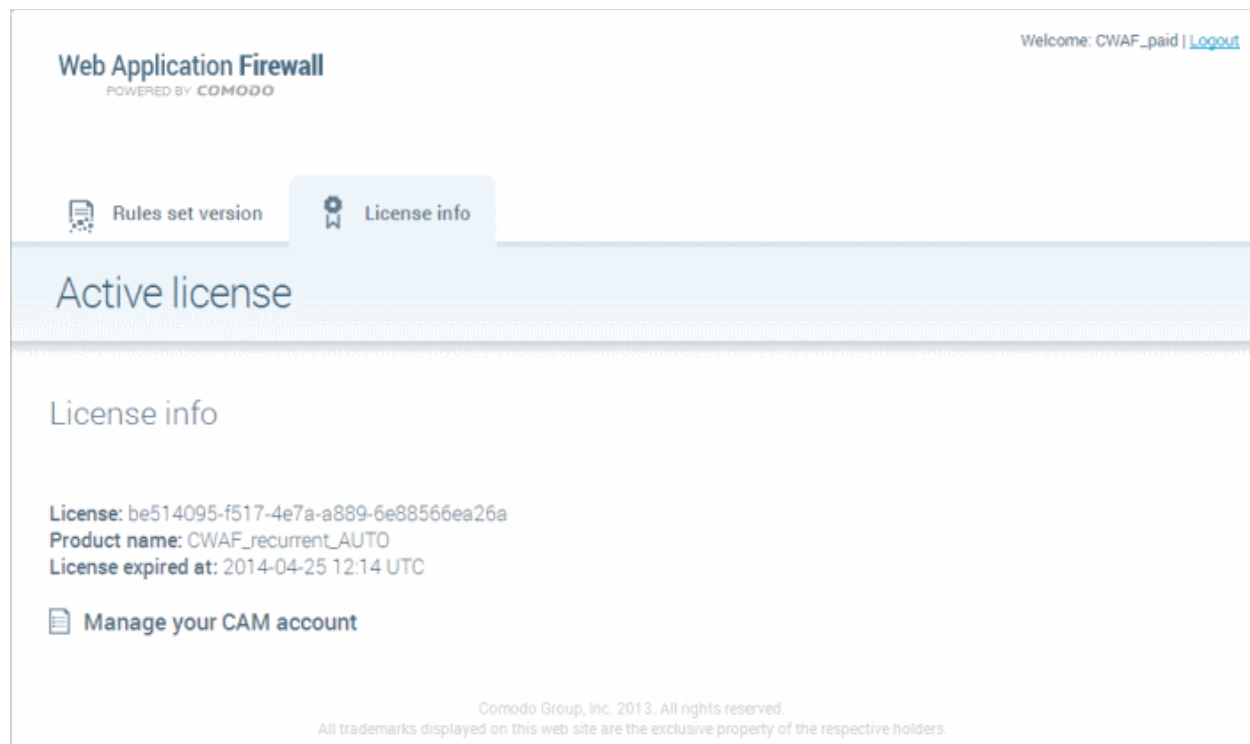
Annotations in the image point to various features:

- Orange box:** The administrator can select the version of the Rule Set to be downloaded (points to the 'Select version' dropdown).
- Green box:** The administrator can select whether to download the full Rule Set or only the updates from the previous version, of the selected version (points to the 'Download full rules set' and 'Download only updates' buttons).
- Red box:** The administrator can download the latest version of the Rule Set or the agent set-up file by clicking the links here (points to the 'Download latest rules set' and 'Download latest installer' links).
- Blue box:** Displays the pre-defined Firewall Rule Sets in the selected version (points to the 'List of rule files' section).
- Yellow box:** The administrator can submit feedback on the selected version by clicking this tab (points to the 'Report a problem with this version' button).

- **Version Management** - The administrator can choose the 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
- **List of rule files** - Displays the firewall rules included in the currently selected rule set version

License Info

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



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 cPanel plug-in on to the server that facilitates the administrator to configure the CWAF implementation

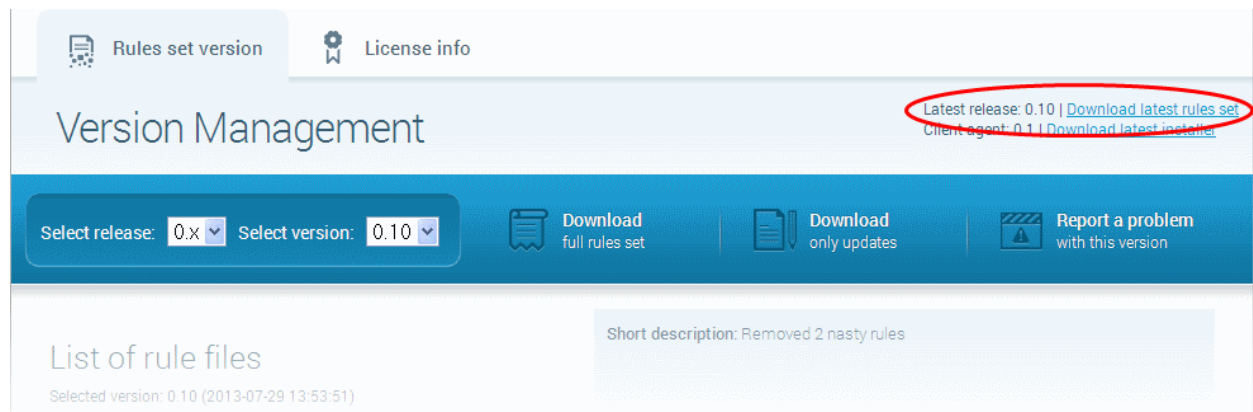
Refer to the following sections for more details on deploying the rulesets:

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

2.1. Downloading and installing rule set packages

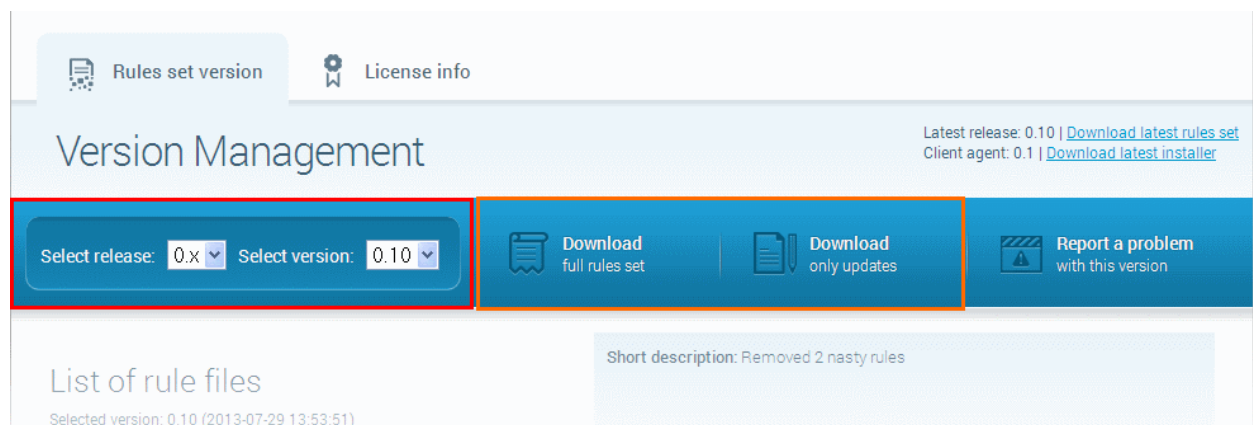
To download the Rule Set

- 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



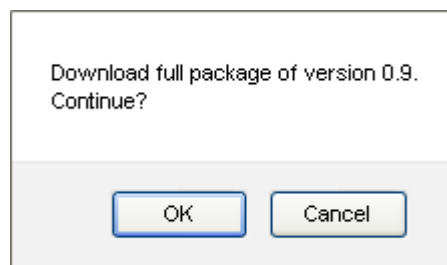
- If you want to download a selected version of the rule set,
 - Select the version from the 'Select version' drop-down
 - select the release number from the 'Select release' drop-down

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.



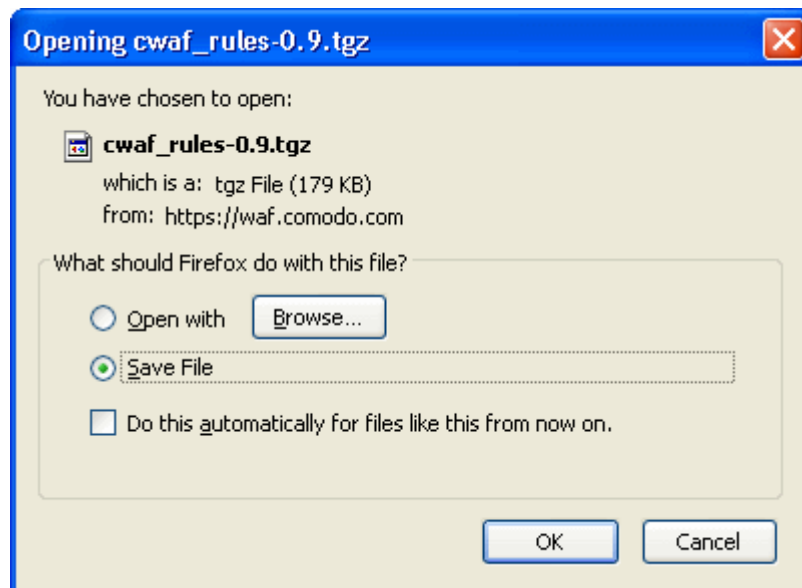
- If you are installing the rule set for the first time, click 'Download full rules set' to download the full set of the selected version.
- If you have already installed the previous version of the rule set and wish to update it to the latest version, click 'Download only updates'

The download confirmation dialog will be displayed



- Click OK

The download dialog will be displayed.



- 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.

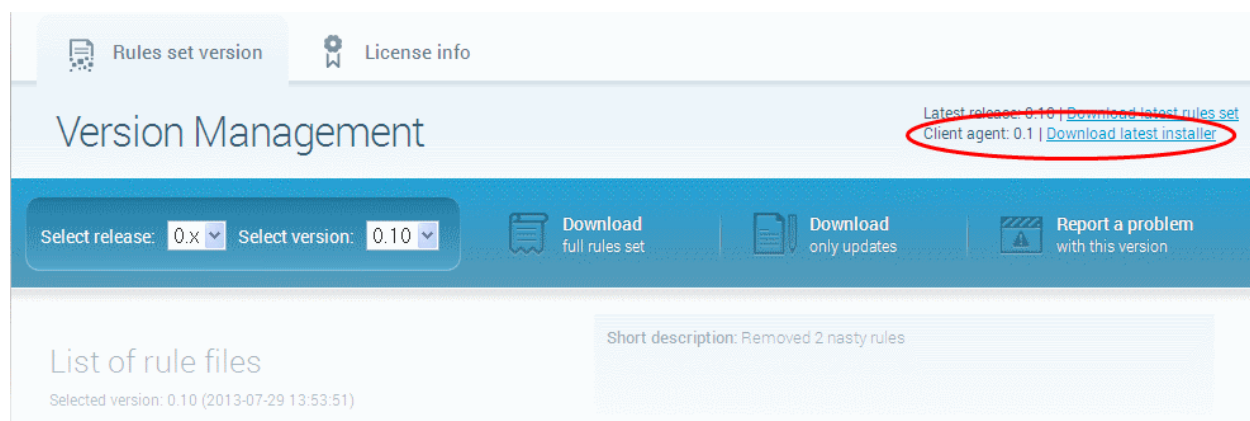
The rule sets in the package will be implemented immediately.

2.2. Using the CWAF Agent

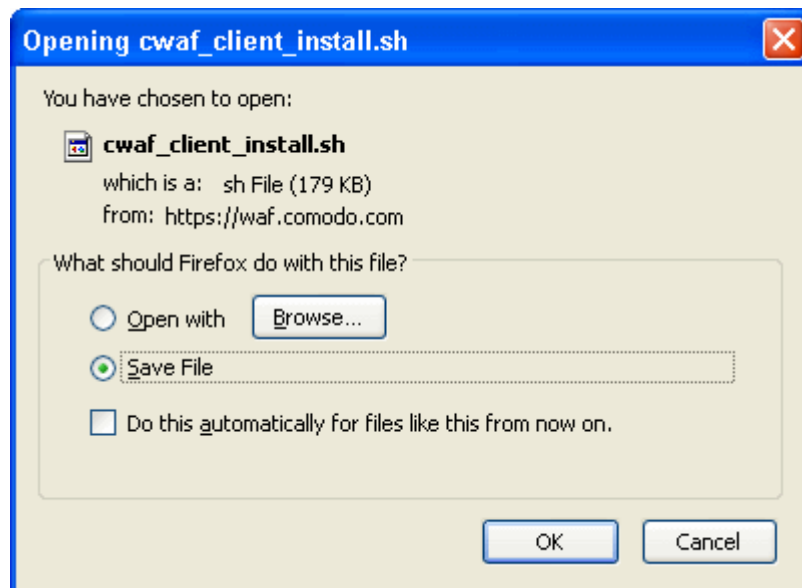
The Comodo Web Application Firewall (CWAF) agent is a small piece of software that can be installed on to the web server to automate the deployment of the periodically published pre-defined set of firewall rule sets on to the web server and to configure the CWAF.

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



The download dialog will appear.



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

You can install the agent in two modes depending on your requirement. Refer to the sections below for more details.

- **Installing the agent for deploying the Rule Sets** - The agent will be installed on the server. The agent will periodically check the CWAF server for updates in the rule sets and automatically download and install the latest rule sets on to the server.
- **Installing the Agent for creating cPanel Plug-in** - The agent will create a cPanel plug-in. The plug-in can be used to configure the behavior of CWAF.

2.2.1. 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 on the server
E.g. `/root`
- Run the installation script with root privileges:
`# bash /root/cwaf_client_install.sh`

Step 1

- Choose the type of installation
Choose type of installation:
1) Cpanel installation
2) Standalone scripts
Choose [1|2]: 1
- To install the agent to download the firewall rule set packages, choose 2

Step 2

- Enter the login credentials for CWAF
Enter CWAF connection data

Enter CWAF user: `jsmith`
Enter CWAF password: `password`

Step 3

- Modify Apache Web Server configuration to enable 'mod_security' module and include CWF Rules, by adding the key 'Include /var/cpanel/cwaf/etc/cwaf.conf' to /usr/local/apache/conf/modsec2.conf

Add this string to Apache HTTPD Mod_security config in your system:

Include "/var/cpanel/cwaf/etc/cwaf.conf"

and reload Apache

Installation complete!

- Restart Apache server

The agent is installed on the server at the path /var/cpanel/cwaf. For more details on configuring CWF using the agent, refer to the section **Using the Agent for Firewall Configuration**.

2.2.2. 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 CWF console tool:

/var/cpanel/cwaf/scripts/updater.pl

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

/var/log/CWF/utls.log

2.2.3. Installing the Agent for cPanel Plug-in

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

Step 1

- Choose the type of installation

Choose type of installation:

1) Cpanel installation

2) Standalone scripts

Choose [1|2]: 2

- To install the agent to create a cPanel plug-in, choose 1

Step 2

- Enter the login credentials for CWF

Enter CWF connection data

Enter CWF user: jsmith

Enter CWF password: password

Step 3

- Modify Apache Web Server configuration to enable 'mod_security' module and include CWF Rules, by adding the key 'Include /var/cpanel/cwaf/etc/cwaf.conf' to /usr/local/apache/conf/modsec2.conf

Add this string to Apache HTTPD Mod_security config in your system:

Include "/var/cpanel/cwaf/etc/cwaf.conf"

and reload Apache

Installation complete!

- Restart Apache server

The agent is installed on the server at `/var/cpanel/cwaf` with a cPanel plugin for CWAF. For more details on configuring CWAF using the plug-in, refer to the section [Using cPanel Plug-in for Firewall Configuration](#).

2.2.4. Using the cPanel Plug-in for Firewall Configuration

CWAF cPanel plug-in allows the administrator to view and modify the web application 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 rule set version.

To access the CWAF cPanel plugin

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

The Comodo Web Application Firewall configuration screen will appear.

Comodo Web Application Firewall

Main	Configuration	Update	Exclude rules	Feedback
Current rules version		2.5 (latest version)		
Apache version		2.2.23		
Mod_security compatible		yes		
Mod_security loaded		yes		
Mod_security conf		/usr/local/apache/conf/modsec2.conf		
Found websites		4		

The interface has five 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
- **Update** - Enables the administrator to manually download the ruleset updates or restore to previous version of rule set. Refer to '[Managing Updates](#)' for more details.
- **Exclude Rules** - Enables the administrator to specify the rules in the currently loaded ruleset to be excluded from implementation. Refer to '[Configuring Exclusions](#)' 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.

Viewing CWAF Information

The Main tab of the CWAF cPanel plug-in configuration screen displays the version details and mod_security configuration of the Apache HTTP server.

Comodo Web Application Firewall

Main	Configuration	Update	Exclude rules	Feedback
Current rules version		2.5 (latest version)		
Apache version		2.2.23		
Mod_security compatible		yes		
Mod_security loaded		yes		
Mod_security conf		/usr/local/apache/conf/modsec2.conf		
Found websites		4		

- **Current rules version** - Displays the version number of the currently loaded rules set
- **Apache version** - Displays the version number of Apache 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.

Configuring CWAF Parameters

The Configuration tab enables the administrator to view and modify the CWAF configuration Parameters.

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	
5	All Warnings from CWAF will be logged.
6	
7	

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

Main
Configuration
Update
Exclude rules
Feedback

System

CWAF main configuration

Debug level:	<input type="text" value="10"/>
Path to log directory:	<input type="text" value="/var/log/CWAF"/>
Debug log:	<input type="text" value="utils.log"/>

CWAF updater configuration

API Login:	<input type="text" value="jsmith"/>
API Password:	<input type="password" value="*****"/>
Rules path:	<input type="text" value="/var/cpanel/cwaf"/>
Exclude conf:	<input type="text" value="etc/cwaf_excluserules.conf"/>

Update config

- **Path to log directory** - 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**)

CWAF updater configuration

- **API 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.
- **API 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.
- **Rules path** - The location at which the rule sets are automatically downloaded for deploying to Mod-security. The administrator can alter this if required. (**Default = /var/cpanel/cwaf/rules**)

- **Exclude conf** - The location at which the rules exclusion configuration is stored. The administrator can alter this if required. (**Default = /etc/cwaf_excluderules.conf**)
- Click Update config to save your changes.

Managing Updates

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

Main	Configuration	Update	Exclude rules	Feedback
Last rules update		0		
Run update script		UPDATE RULES		
Restore previous rules		RESTORE RULES		

- To update the rule set to the latest version, click UPDATE RULES

Main	Configuration	Update	Exclude rules	Feedback
Last rules update		0		
Run update script		UPDATE RULES		
Restore previous rules				

Updater status:
01/08/13 10:49:04 updater[7570] debug is ON, level = 10
01/08/13 10:49:04 updater[7570] create pid file
01/08/13 10:49:04 updater[7570] lwp_params: timeout=60 sec, save_to_file flag: 1
01/08/13 10:49:04 updater[7570] installed latest version, update not need
01/08/13 10:49:04 updater[7570] update script ends work!

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

- To Restore the rule set to the previous version, click RESTORE RULES



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:

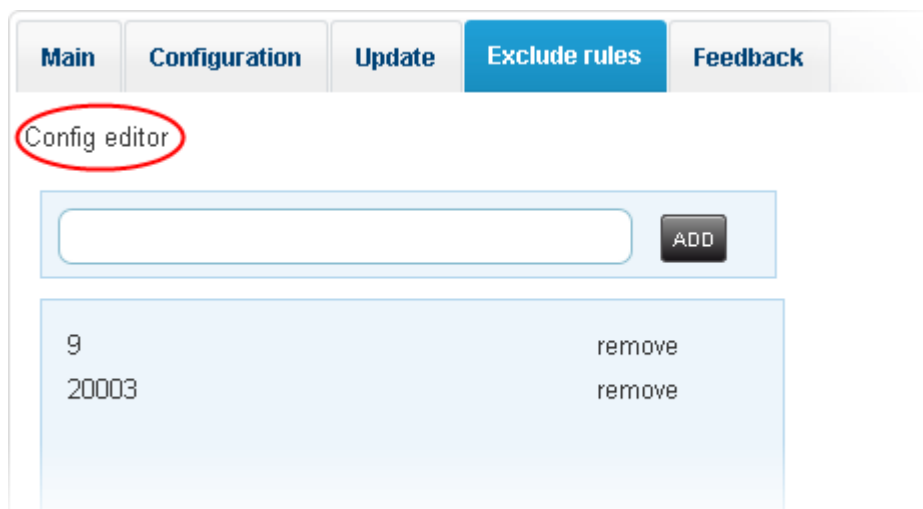
`/var/log/CWAF/utlis.log`

Configuring Exclusions

The Exclude rules tab allows the administrator to specify the rules to be excluded from implementation from the currently loaded rule set. The interface is presented in two modes

- **Simple Mode**
- **Config Editor Mode**

The administrator can switch between the modes by clicking the respective links at the top left.



Simple Editor Mode

The administrator can specify a single rule, a list of rules or a range of rules to be excluded in the simple mode.

To add the rule(s) to be excluded

- Enter the rule id in the text box
 - For a single rule, enter the id of the rule (E.g. 1000)
 - For a list of rules, enter their ids separated by comma (E.g. 1000, 1050, 1075)
 - For a range of rules, enter the first and last ids separated by an hyphen (E.g. 1000-2000)

For guidance on identifying the rule IDs for the rules to be excluded, refer to the **Appendix 1 – Identifying Rule IDs for Exclusion**

- Click 'ADD'
- Repeat the process for adding more exclusions
- Click 'Save configuration' for your configuration to take effect.

- Restart the Apache service.

The rule(s) will be added to the exclusions.

Configuration Editor Mode

The Configuration Editor mode opens a configuration editor window that allows the administrator to enter the configuration key for excluding the rule(s).

To add the rule(s) to be excluded

- Enter the configuration keys for excluding the rules by specifying their IDs in the text box

The screenshot shows the 'Configuration Editor' window with the 'Exclude rules' tab selected. The 'Simple editor' section contains a text box with the following text:

```
SecRuleRemoveById 9  
SecRuleRemoveById 20003
```

Below the text box is a blue 'Save' button.

- Click 'Save' for the keys to take effect.
- Restart the Apache service.

Sending Feedback

The Feedback tab allows the administrator to post feedback on the currently loaded rule set to Comodo. The experts at Comodo will analyze the feedback and use them to correct and enhance the rule set for the next version.

The screenshot shows the 'Feedback' tab in the Configuration Editor. It contains the following fields:

- Rules version:** A text box containing '2.5'.
- Rule id(optional):** A text box containing '10289'.
- Type:** A dropdown menu with 'False positive' selected.
- Message:** A text box containing the text: 'The url example.com is not allowed by the rule, in spite of it being a trustworthy site.'

At the bottom of the form is a blue 'Send feedback' button.

- **Rules version** - The version number of the currently loaded rule set. This field will be auto populated.
- **Rule id** - The administrator can enter the ID number of the specific rule upon which feedback is provided. This field is optional.
- **Type** - The administrator can select the type of the issue to be reported from the drop-down
- **Message** - The administrator can enter the feedback message
- Click 'Send feedback' to submit your feedback to Comodo.

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

2.2.5. Uninstalling the CWAF Agent

The CWAF is installed at the path `/var/cpanel/cwaf` by default.

To uninstall CWAF Agent,

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

Do you want to remove Comodo WAF application?

Enter answer [y/n] y

*Please don't forget to remove string "Include /var/cpanel/cwaf/etc/cwaf.conf" from file
/usr/local/apache/conf/modsec2.conf*

and reload Apache

Comodo WAF uninstalled!

- Remove the string `'include /var/cpanel/cwaf/etc/cwaf.conf'` from the file `'/usr/local/apache/conf/modsec2.conf'`
- Reload 'Apache'

The agent will be removed from the server.

2.3. Reporting Problems to Comodo

The feedback from the administrators provide a key role in developing and improvising the Firewall Rule Sets released in successive versions. Comodo welcomes the views, comments, ideas and reports on issues faced from the administrators as their feedback. The feedback can also be used to notify any false positives reported by the firewall. The feedback will be appreciated and implemented in the next version of the rule set, if found appropriate.

The 'Report a problem' tab enables the administrator to post feedback and report problems on the currently loaded rule set.

To send a feedback

- Click on the 'Report a problem' tab

Web Application Firewall
POWERED BY COMODO

Welcome: jsmith | [Logout](#)

[Rules set version](#) [License info](#)

Version Management

Latest release: 0.10 | [Download latest rules set](#)
Client agent: 0.1 | [Download latest installer](#)

Select release: 0.x Select version: 0.10

[Download full rules set](#) [Download only updates](#) [Report a problem with this version](#)

Error feedback

Reason
rule gives false positive

Rule ID (optional)
Number only...

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

[Send report](#)

List of rule files

Selected version: 0.10 (2013-07-29 13:53:51)

File Name	Status
bL_domains	unmodified
bL_malwares	unmodified

- **Reason** - Enables the administrator to choose the subject for the feedback.
- **Rule ID** - The administrator can enter the ID number of the specific rule upon which feedback is provided. This field is optional.
- **Description** - The administration can enter a description of the problem. In order for thorough analysis of the problem the administrator is advised to provide the system configuration and the event logs, along with details of the problem.
- Enter the details as described above and click 'Send report'. The report will be immediately sent to Comodo.

Error feedback

Reason

- rule gives false positive
- rule gives false positive
- rule seems doesn't work
- other

3.Managing CWAF License

The administrator can view the license information of the CWAF account and the expiration date from the 'License Info' tab. The interface also provides a shortcut to login to Comodo Accounts Manager (CAM) account if the administrator needs to renew or upgrade the license.

The screenshot displays the 'Web Application Firewall' interface, powered by Comodo. At the top right, it says 'Welcome: jsmith | [Logout](#)'. Below the header, there are two tabs: 'Rules set version' and 'License info', with the latter being selected. The main content area is titled 'Active license' and contains a 'License info' section. This section lists the following details: 'License: [REDACTED]', 'Product name: CWAF_recurrent_AUTO', and 'License expired at: 2014-04-25 12:14 UTC'. Below this, there is a link 'Manage your CAM account' with a document icon. At the bottom of the page, a footer states: '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 license key of the CWAF account.
- **Product name** - Displays the CWAF product subscribed for.
- **License expired at** - Displays the expiration date of the license.
- **Manage your CAM account** - Takes you to your account page at <https://accounts.comodo.com>. The account page enables you to renew or upgrade your license and to subscribe for other Comodo products and services.

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

The screenshot shows the 'Active license' section of the Comodo Web Application Firewall Admin Guide. The 'License info' section displays the following details:

- License: be514095-f517-4e7a-a889-6e88566ea26a
- Product name: CWAF_recurrent_AUTO
- License expired at: 2014-04-25 12:14 UTC

The 'Manage your CAM account' link is circled in red. A red arrow points from this link to the 'Subscriptions' table in the 'Manage Subscriptions' page.

The 'Manage Subscriptions' page shows the following information:

- Current Bonus Balance: \$4.40 USD
- Welcome: Test Paid
- Navigation: WebInspector | Comodo Membership | Comodo Web Application Firewall | My Account | Help | Contacts | Logout
- Search: Search | Create New | Manage Subscriptions
- Subscriptions Table:

Product name	License key	Expired At	Status	
CWAF_recurrent_AUTO	be514095-f517-4e7a-a889-6e88566ea26a	2014-04-25	VALID	View

1 Found

CAM v.6.2.19466

[Svn Information](#)

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 plugin by specifying their rule IDs. Please refer to the section [Using the cPanel Plug-in for Firewall Configuration](#) > '[Configuring Exclusions](#)' for more details.

This section explains on how to identify the Rule IDs for the rules to be excluded.

To exclude a rule that is not needed

- 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/rule-CVE-2012-0021.conf` is shown below:

```
SecRule REQUEST_HEADERS:Cookie "@rx ^(.*)*=(:.*)*$" "phase:1,log,deny,status:403,msg:'CVE-2012-0021 attack',id:20003"
```

- Get the rule ID from the string.

In the example above, the rule ID is '20003'

- Use this ID to add the rule to the exclusion list, as explained in the section [Using the cPanel Plug-in for Firewall Configuration](#) > '[Configuring Exclusions](#)'.

If the administrator identifies that a rule is behaving incorrectly for their web site, such as blocking of certain web pages, the administrator can identify the rule directly 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"]

The administrator can identify the rule ID for the incorrectly behaving rule from the error log and use it to specify the rule to be excluded as explained in the section [Using the cPanel Plug-in for Firewall Configuration](#) > '[Configuring Exclusions](#)'.

- In the above example, the rule ID is "801448"

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

STE 100

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>.