COMODO
Creating Trust Online®

Web Application Firewall
POWERED BY COMODO

Comodo
Web Application Firewall

Software Version 2.24

Administrator Guide

Guide Version 2.24.010620

Comodo Security Solutions
1255 Broad Street
Clifton, NJ 07013

Table of Contents

1. Comodo Free ModSecurity Rules - Introduction

Web applications are arguably the most important back-end component of any online business. They are used to power many of the features most of us take for granted on a website, including web-mail, online stores, software-as-a-service, payment gateways, forums, dynamic content, social media functionality and much more. A security breach on a web application can have potentially devastating implications for the site owner, including site downtime, loss of corporate data and even theft of confidential customer information. It is therefore of paramount importance that web applications are kept strongly protected against attack at all times. **Comodo Web Application Firewall** (CWAF) provides powerful, real-time protection for web applications and websites running on 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 **'Linux - Install 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
  - **Sign up for Web Application Firewall** – Help to sign-up for the product
  - **Login to the Administration Console** – Help to log-in to the web admin console
  - **The Admin Console - Main Interface** - Description of the web administration console
- **Deploy CWAF rules on Server** - Guidance on downloading and deploying the firewall rule sets on to the server

- **Linux - Install the Agent and Control Panel Plugin** - Help to download and deploy the firewall rule sets on Linux
  - **Linux - Install the Agent in Standalone Mode**
- **Windows - Install the Ruleset on Windows IIS** - Help to download and deploy the firewall rule sets on Windows
- **Use the Web Hosting Control Panel Plugin for Firewall Configuration** - Help to configure firewall rules and update rule sets
- **Use 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
- **Uninstall CWAF** - Help to remove CWAF from the web hosting control panel plugin
- **Download and Install Rule Set Packages** – Help to manually download and deploy the firewall rule sets
- **Report Problems to Comodo** - Post feedback to Comodo
- **Submit Tickets to Comodo** – Report issues to Comodo

- **Manage CWAF License** – Help to view and manage CWAF licenses, and to subscribe for other Comodo products and services
- **CVE Coverage Information** – Help 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

You can download CWAF from Comodo Accounts Manager at **https://accounts.comodo.com/cwaf/management/signup**.

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 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*

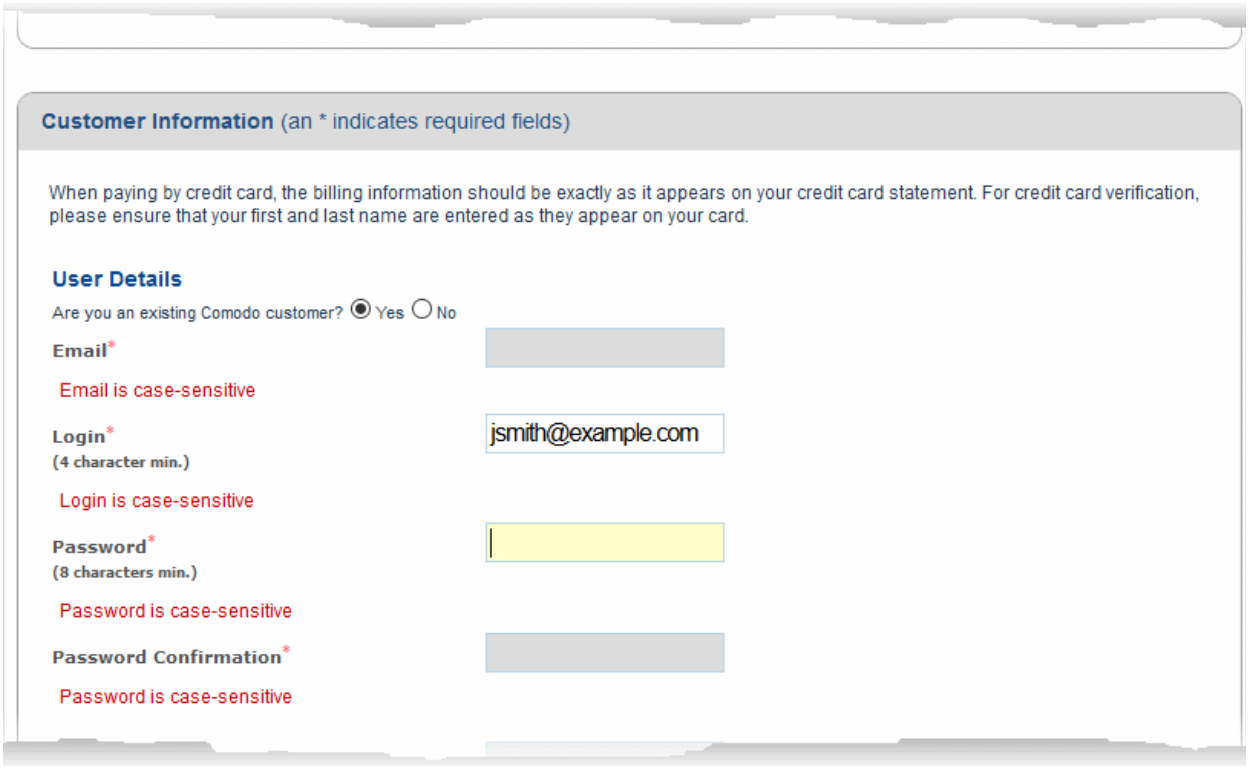
Country* United States

State or Province -Unknown-

Postal Code*

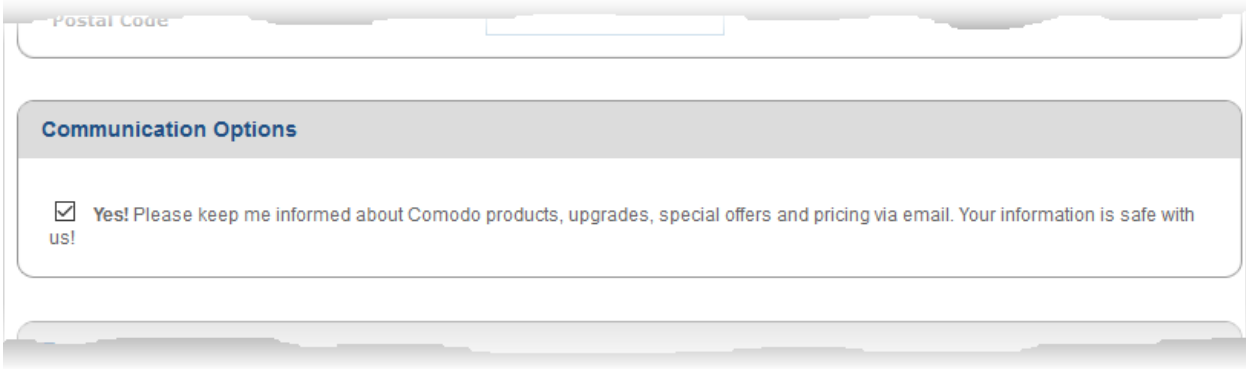
Communication Options

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



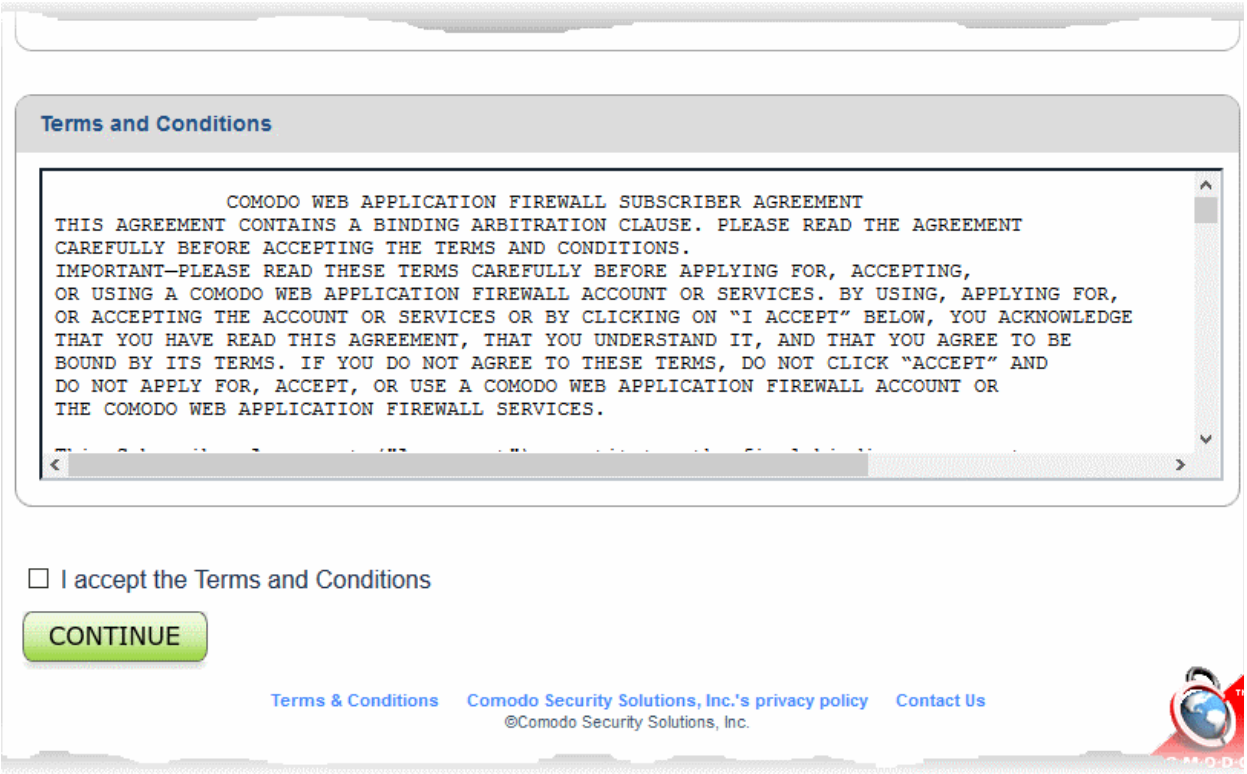
Communication Options:

- 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.



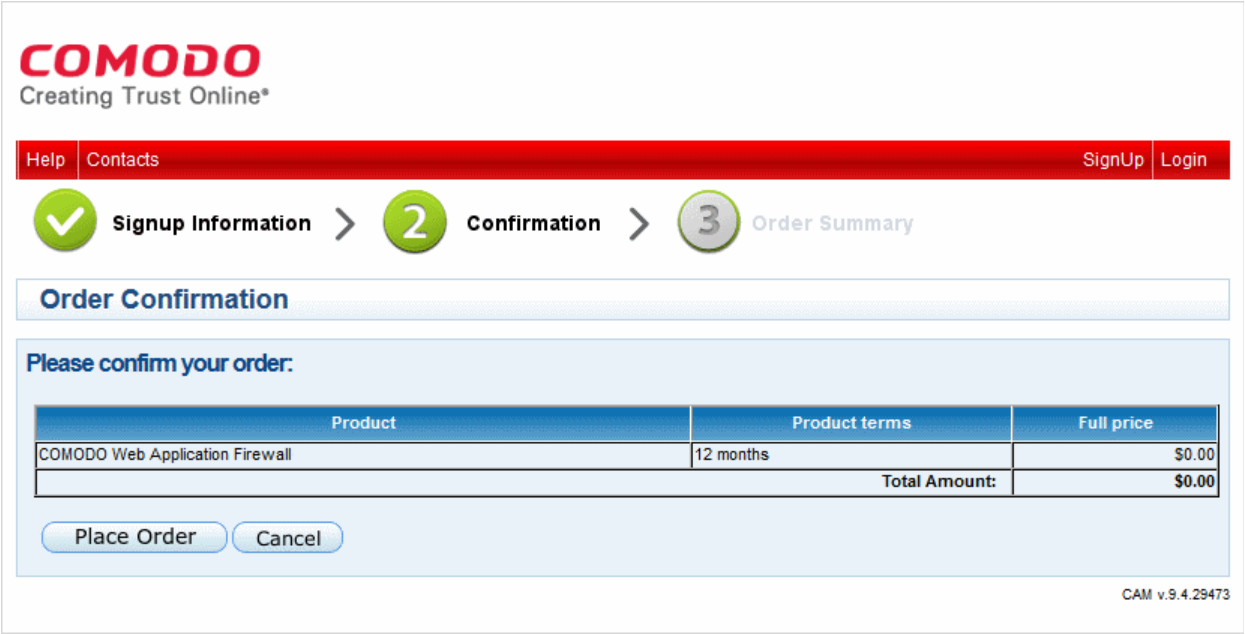
Terms and Conditions:

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



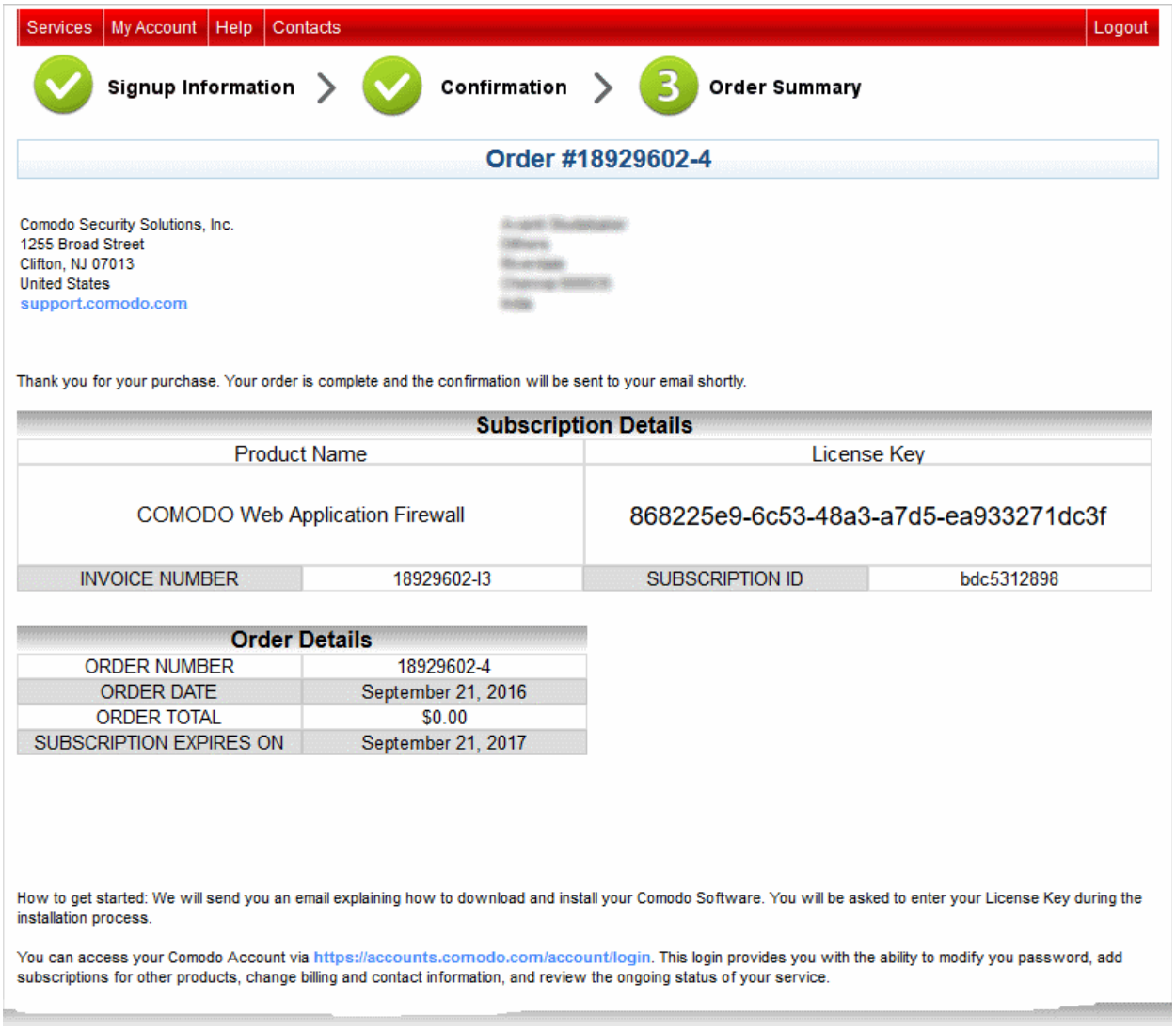
- Click 'Continue'

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.



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

Further Read:

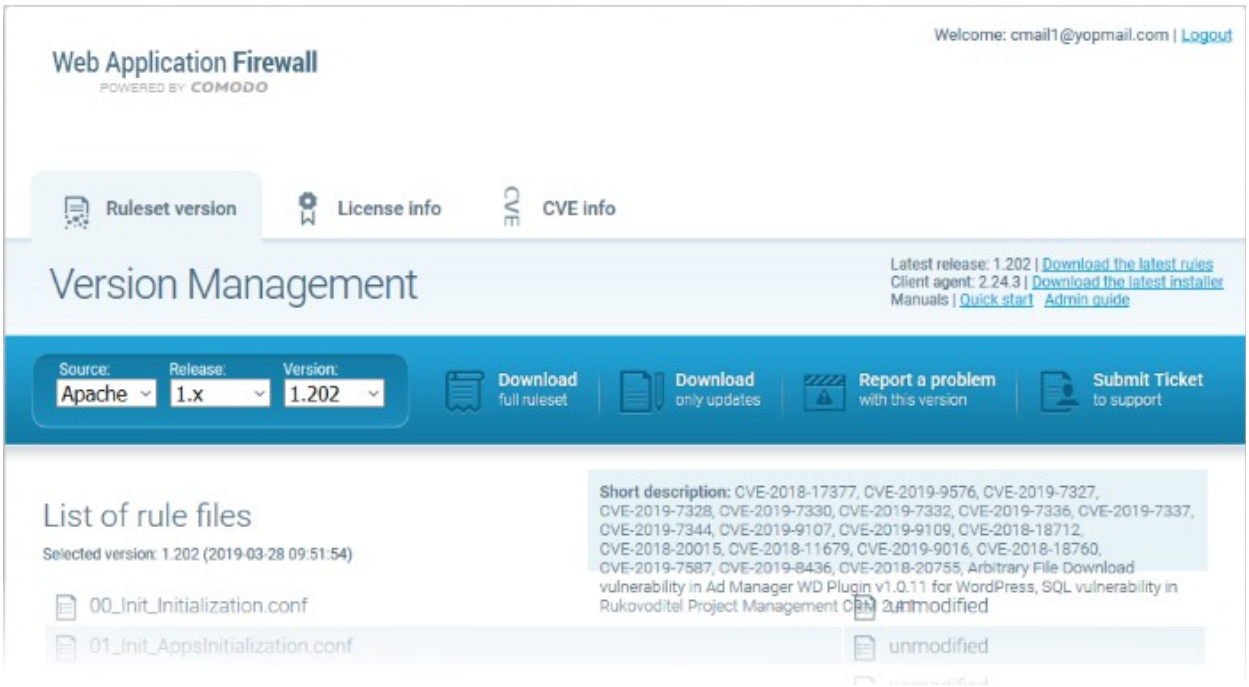
- **Log-in to the Administration Console**
- **Deploy CWAF rules on Server**

1.3. Login to the Administration Console

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

- Enter the username and password you created at signup
- Click 'Login'

You will be taken to the CWAF web admin console:



1.4. The Admin Console - Main Interface

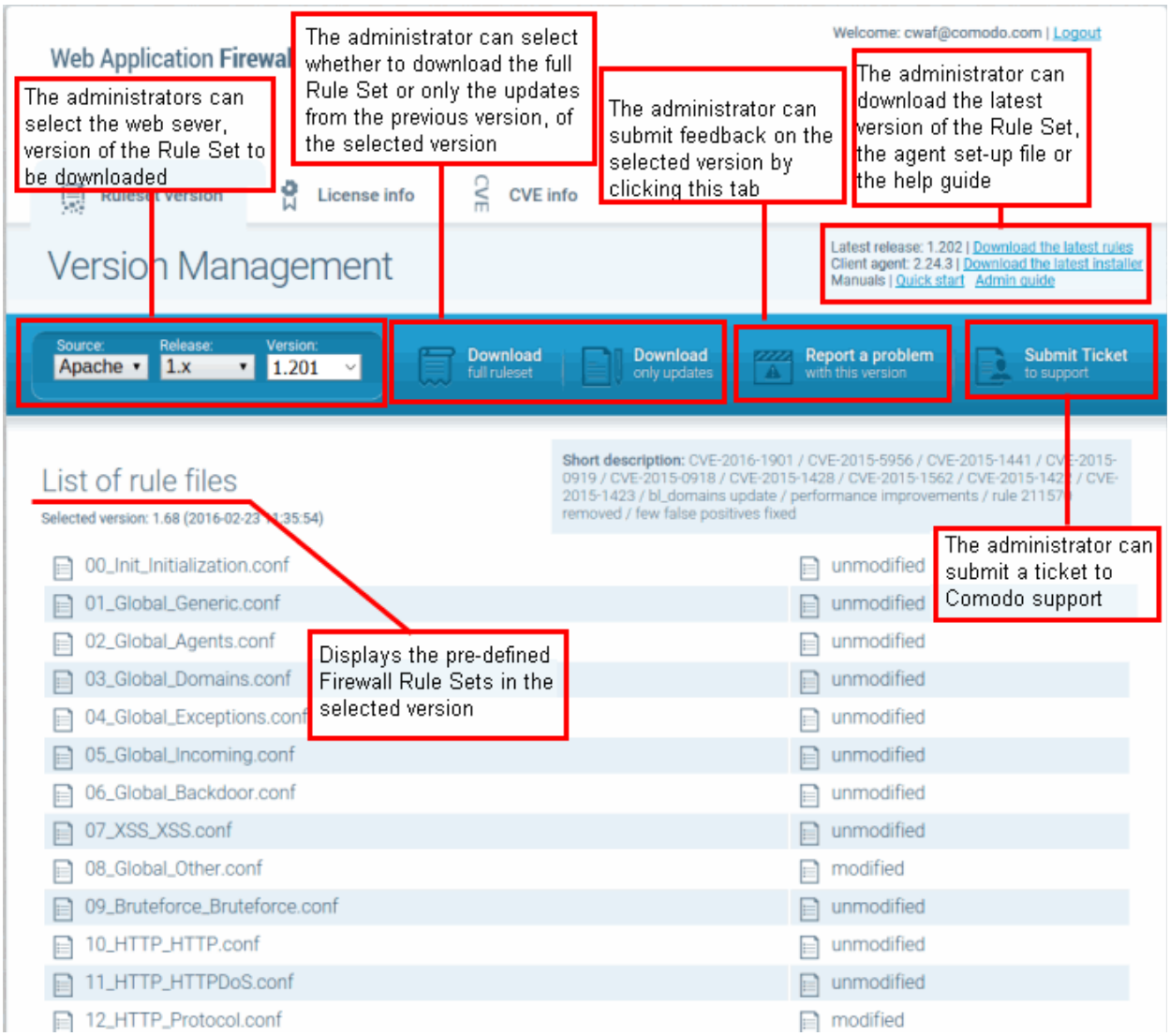
- Comodo Web Application Firewall (CWAF) uses pre-defined rule-sets to control inbound and outbound traffic to/from web apps.
- The admin console lets admins download these rule-sets and deploy them on their web application servers.
- Linux users can also install an agent that will automatically download and update the rule-sets when required.
- The agent can also install CWAF plugins for popular control panels (cPanel, Plesk, DirectAdmin and Webmin).

The admin interface has two tabs:

- **Rule Set Version**
- **License Info**

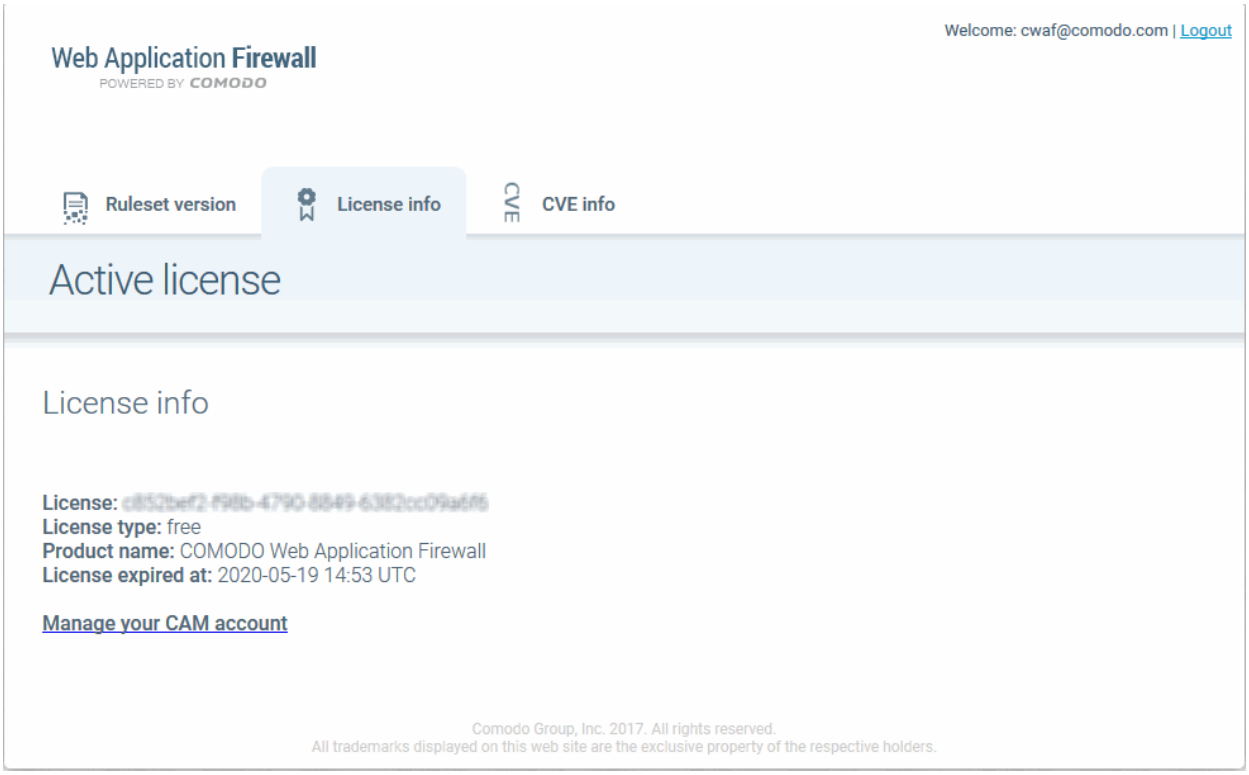
Rule Set Version

Download the ruleset version or agent you require from this interface:



License Info

The license info tab shows your account license key, license type and license expiry date. The interface also has a link to Comodo Accounts Manager where you can renew or upgrade the license.



2. Deploy CWAF Rules On Server

- Comodo Web Application Firewall allows or denies access to a web-app based on firewall rule sets.
- Rule sets are made up from one or more individual firewall rules. Each rule 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 rule sets which can be downloaded from the CWAF console.
- Linux admins can automatically implement the latest rules by installing the CWAF Agent.

The agent can be configured to:

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

See the following sections for more details on deploying the rulesets:

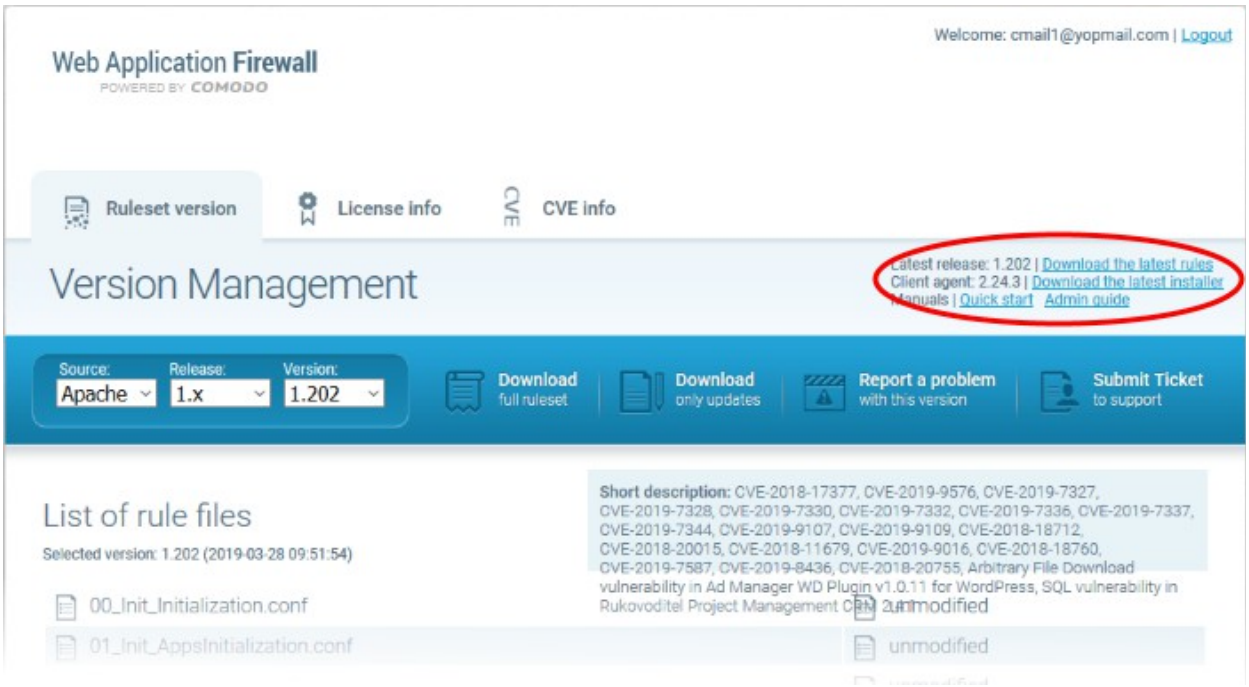
- **Linux - Install the Agent and Control Panel Plugin**
- **Windows - Install the Ruleset on Windows IIS**
- **Download and install Ruleset package**

2.1. Linux - Install the Agent and Control Panel Plugin

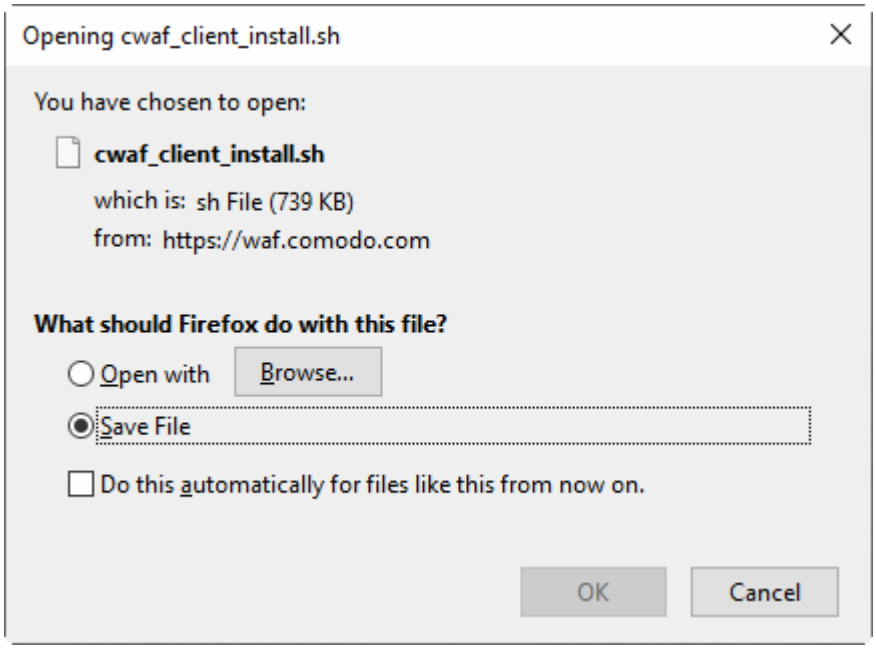
The CWAF agent can automate the deployment of firewall rule sets.

Download the CWAF agent installation file

- Log-in to the web admin 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 the web server type (Apache, LiteSpeed or Nginx), and any for installed control panels (cPanel, Plesk, DirectAdmin, Webmin).

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 CWAF Agent will check to identify the web-server type and version:

1) Check for Apache and its version:

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

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

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

2) Check for LiteSpeed and LiteSpeed mod_security:

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

3) Check for Nginx:

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

4) Checking for prerequisites:

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

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

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

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

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

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

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

6) Check for required Perl modules:

CWAF will check for Perl modules and install them if required

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

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

Click 'No' to decline Perl modules auto-installation. The following message will be displayed:"Please install perl modules [PERL MISSED MODULES] manually and run installation script again"

If problems were detected, the warning message will be displayed: "CPAN is not configured! Please run [CPAN BIN] and configure it manually, then rerun this installation"

After successful installation, the following message will be displayed: "DONE, PRESS ENTER":

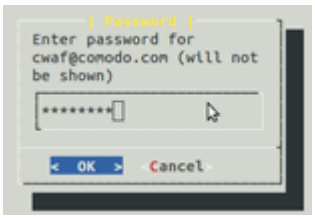
Step 2

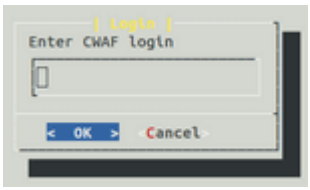
Select the web platform:

- If multiple web servers are found, select the one you prefer. The following message will be displayed: "Please select your WEB platform". Otherwise, the following warning will be displayed: "WEB platform is not selected"
- If the selected web platform isn't supported, the following warning message will be displayed "Selected WEB platform [PLATFORM] is not supported" and installation will be terminated.

Step 3

- Enter login credentials for Comodo Web Application Firewall





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, see the section **Use Web Host Control Panel plugin for Firewall Configuration.**

2.2. Linux - Install the Agent in Standalone Mode

Install the agent on 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-host control panel is found, the agent will be installed in standalone mode. The installation steps for standalone mode are the same as for the plug-in. See **Install the Web Host 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 CWAF Rules, by adding the key '*Include <CWAF_INSTALL_PATH>/etc/cwaf.conf*' to the *'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.

The agent, in this example, is installed on the server at the path */opt/cwaf*. For more details on configuring CWAF using the agent, see **Use 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

Install Mod-Security

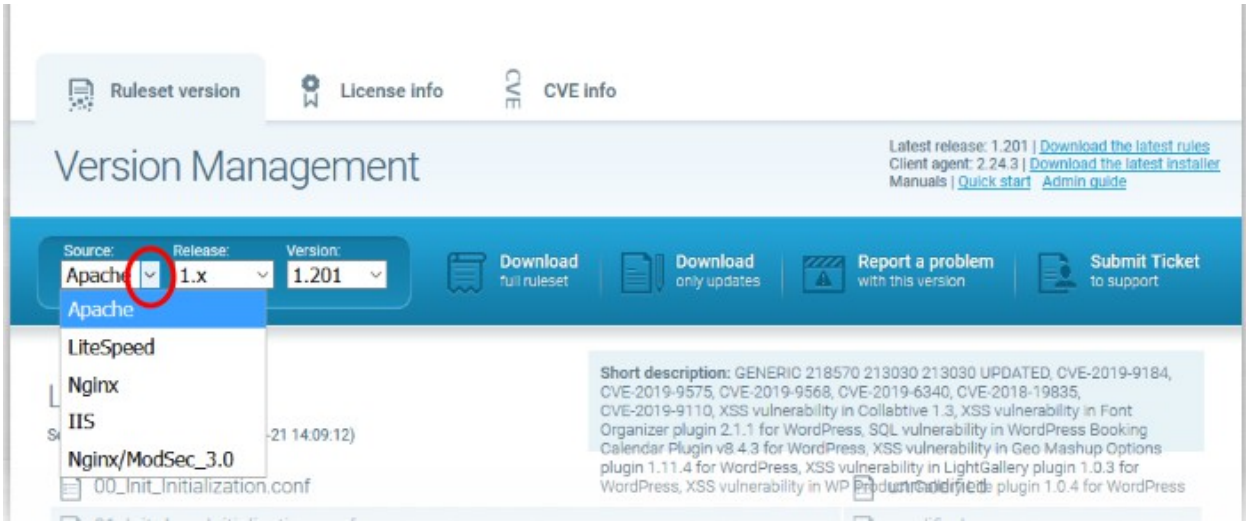
- Download and run the **Mod_security installer**

  Mod_security can be included on any website. Add the following line to the web.config file > system.webServer section:

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

Download and install CWAF rules

- Log-in to the web admin 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.

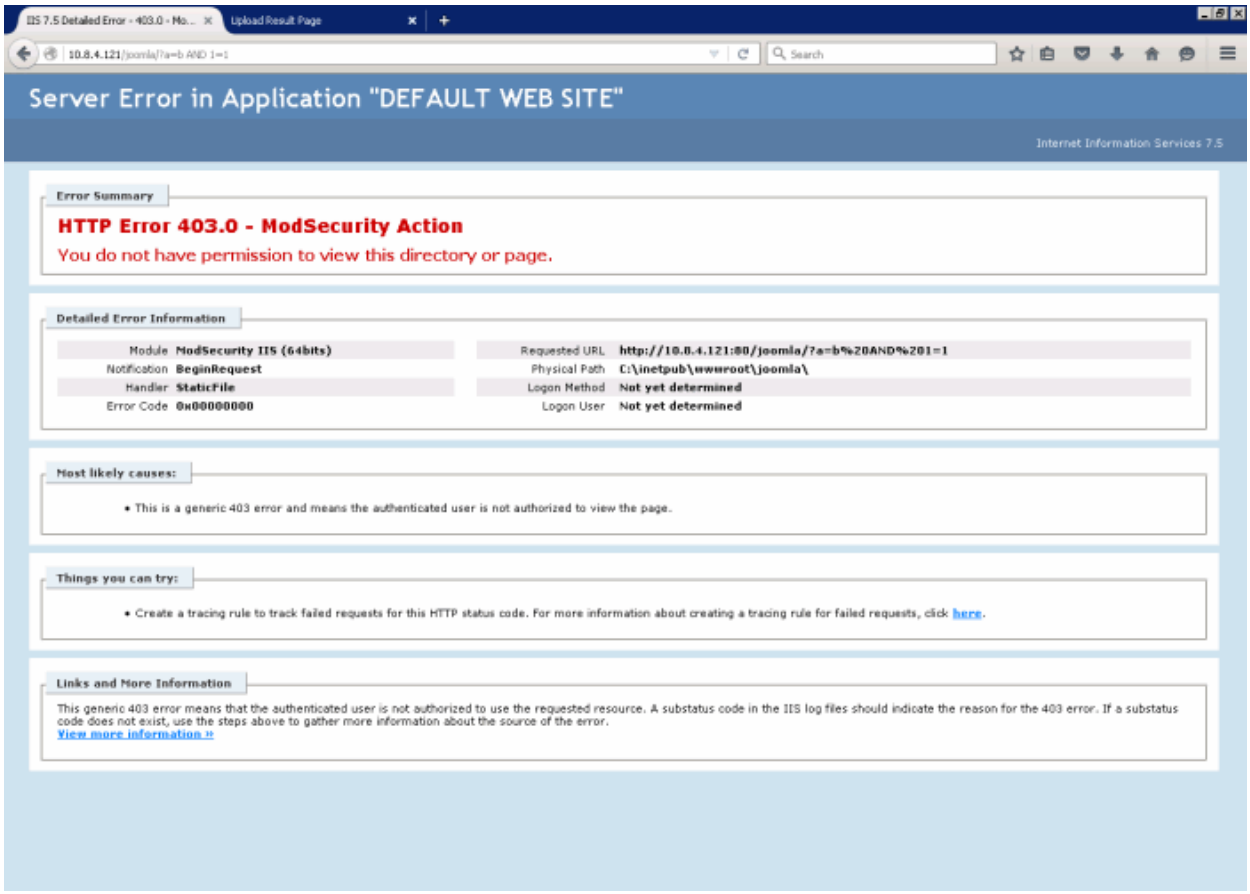


- Click 'Download full ruleset'
- Navigate to “C:\Program Files\ModSecurity IIS” and save the .zip file
- Extract to “C:\Program Files\"
- Restart IIS

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 control panel plugins let you control the firewall using your favorite control panel.

Access the CWAF cPanel plugin

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

Access the CWAF DirectAdmin plugin

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

Access the CWAF Plesk plugin

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

Access the CWAF Webmin plugin

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

The Comodo Web Application Firewall configuration screen appears:

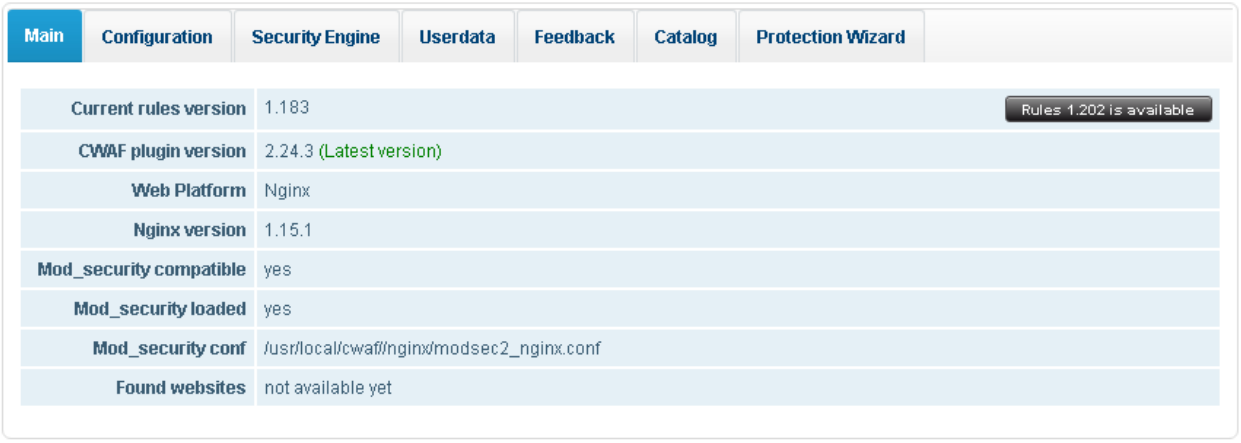
The interface has eight tabs:

- **Main** – Version number of the currently loaded rule set, Apache server, mod-Security status, and number of **websites protected**. See '**View CWAF Information**' for more details
- **Configuration** - View and edit CWAF configuration parameters. See '**Configure CWAF Parameters**' for more details
- **Security Engine** - Set up rules for the Mod_security option. See '**Manage Security Engine**' for more details
- **Userdata** – Manage custom user settings, such as user rules, Mod_security options, and currently loaded rule-sets. See '**Configure Userdata**' for more details.
- **Feedback** – Submit comments and suggestions on the product. See '**Send Feedback**' for more details.
- **Catalog** - Specify rules that should be excluded from your deployment. See '**Manage Catalog**' for more details.
- **Protection Wizard** – Enable/disable rules depending on the specific web applications installed on your server. See '**Protection Wizard**' for more details.

2.4.1. View and Update CWAF Information

- The 'Main' tab in the CWAF web host control panel plugin contains general version and compatibility information about your deployment.
- You can also download the latest rules from this interface

Web Application Firewall | Free ModSecurity Rules from Comodo

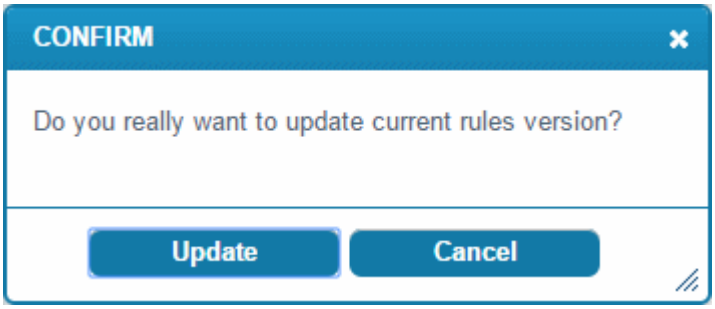


- **Current rules version** - The rule set version that you have installed.
- **CWAF plugin version** – The version of the plugin that you have installed.
- **Web Platform** – The type of web server you have installed
- **<webserver> version** - The version number of the web server you have installed
- **Mod_security compatible** – States whether or not your web-server and version are compatible with the mod_security rules used by the firewall.
- **Mod_security loaded** - States whether mod-security rules are currently active on your server
- **Mod_security conf** - Location of mod_security configuration file for your web-server type.
- **Found websites** – Lists the number of sites hosted on the web-server

Download the latest rule set version

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

A confirmation message is shown:



- Click 'Update'.

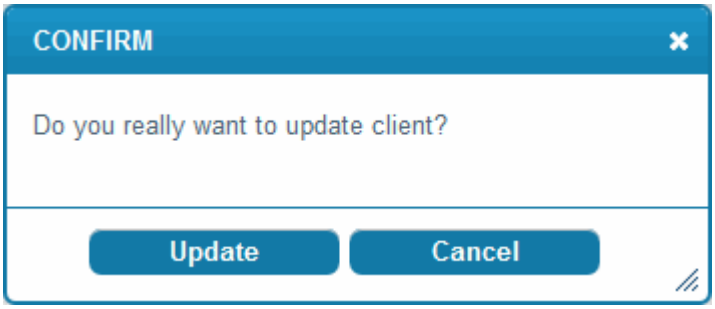
The updater will automatically download and deploy the latest version of the rule set.

Wait till the page has reloaded. The 'Current rules version' will update as follows:

Update the CWAF plugin to the latest version

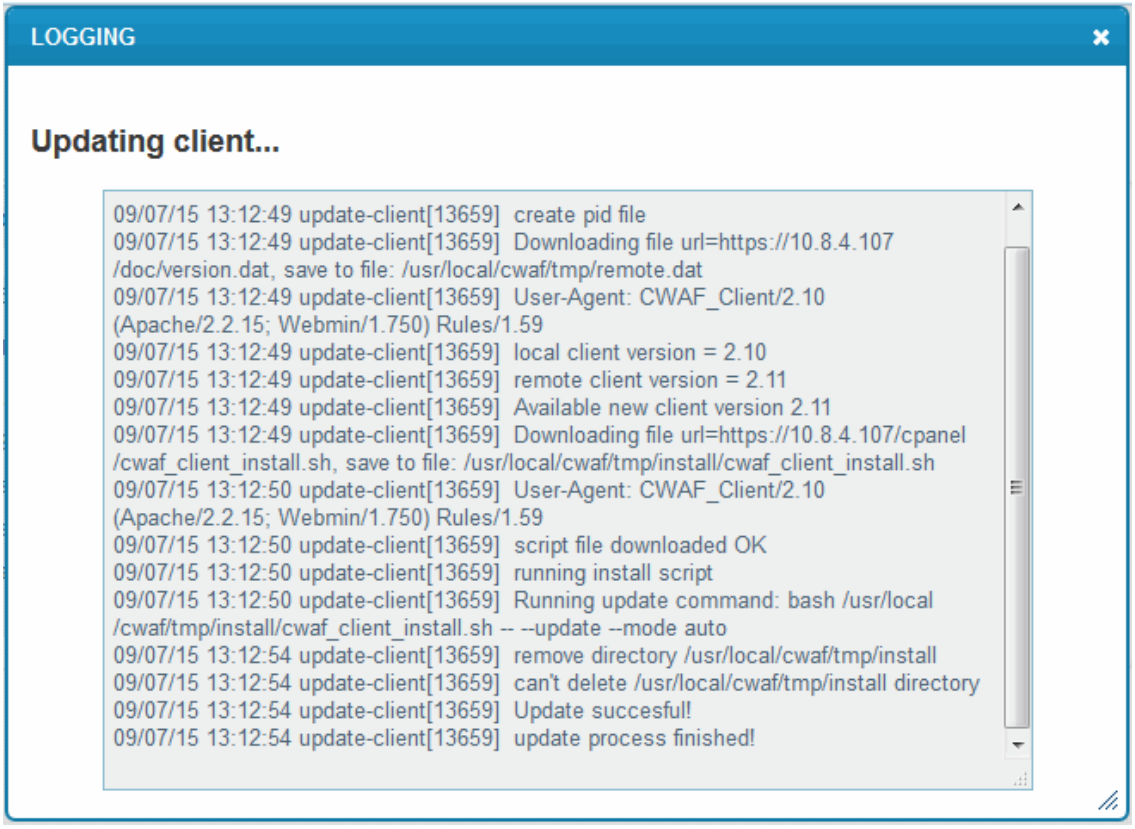
- Login to cPanel on your server
- Click 'Plugins' > 'Comodo WAF' > 'Main'
- Click 'Client X.X is available' at the far-right of the screen:

A confirmation is shown as follows:



- Click 'Update'

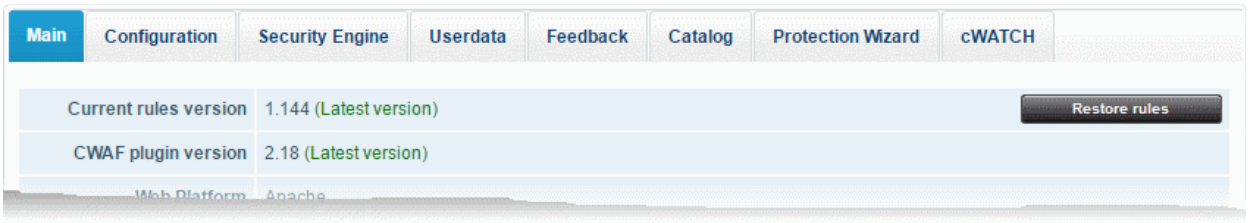
The updater will automatically download and install the latest version of the plugin:



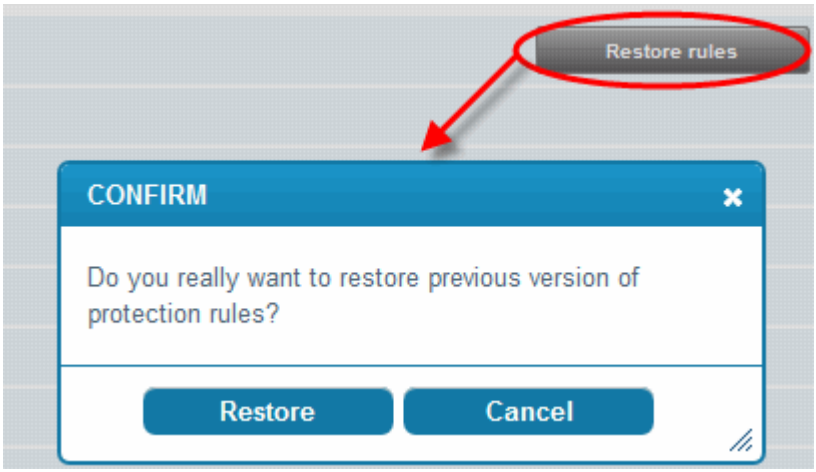
Restore the rule set to the previous version

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

- Click 'Restore rules' at the far-right of the screen:



A confirmation appears as follows:



- Click 'Restore'

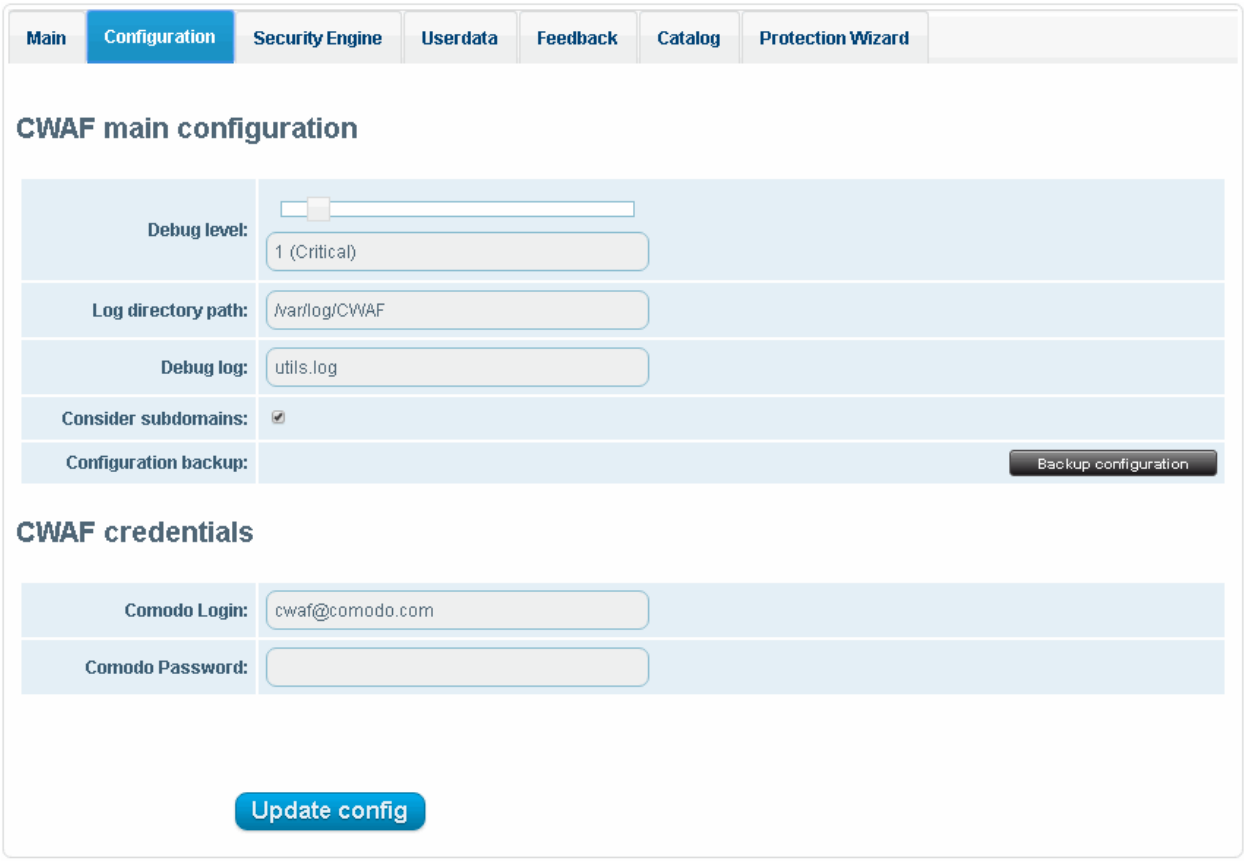
The agent will revert the last update and restore the previous version of the rule set in the Mod_Security firewall.

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

  /var/log/CWAF/utils.log

2.4.2. Configure CWAF Parameters

The configuration tab lets you view and modify various CWAF settings.



CWAF main configuration

- **Debug level** - The slider lets you set how comprehensively CWAF should log events.
  - The higher the level, the more types of event are captured. Default = 0 – No events logged.
  - The following table is a rough guide to the events captured at each setting.

Level	Description
0	No events are logged.
1	Only critical events are logged.
2	
3	
4	CWAF logs all critical and non-critical security warnings.
5	
6	
7	
8	Notifications of all types are logged.
9	
10	Every event is logged.

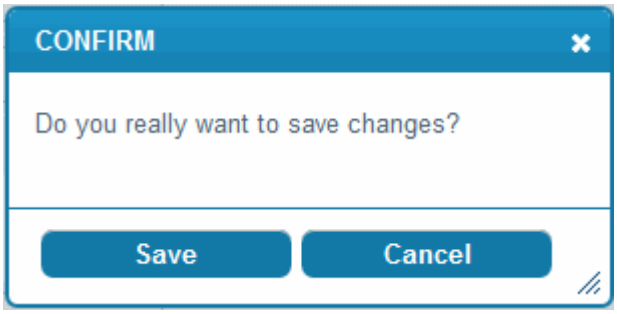
- **Log directory path** - Edit the location at which the CWAF log file is stored. (***Default: /var/log/CWAF***)
- **Debug log** - The name of the log file (***Default: utils.log***)
- **Consider subdomains** - Specify whether CWAF should log events on sub-domains of your domain. (*.domain.com)
- **Configuration backup -** Save a copy of your current configuration. The backup covers debug level, log directory path, login credentials, userdata and excluded rules list. You can also restore your CWAF configuration if required.

CWAF credentials

- **Comodo Login** - The user name of the CWAF account. This field is pre-populated with the username specified when installing the agent. If you have changed your credentials for any reason, then please enter them here so the CWAF agent can login and download the latest rule sets.
- **Comodo Password** - The password for the CWAF account. See above.

Note: DirectAdmin users - The **Feedback** feature is only available if you have provided credentials in these fields.

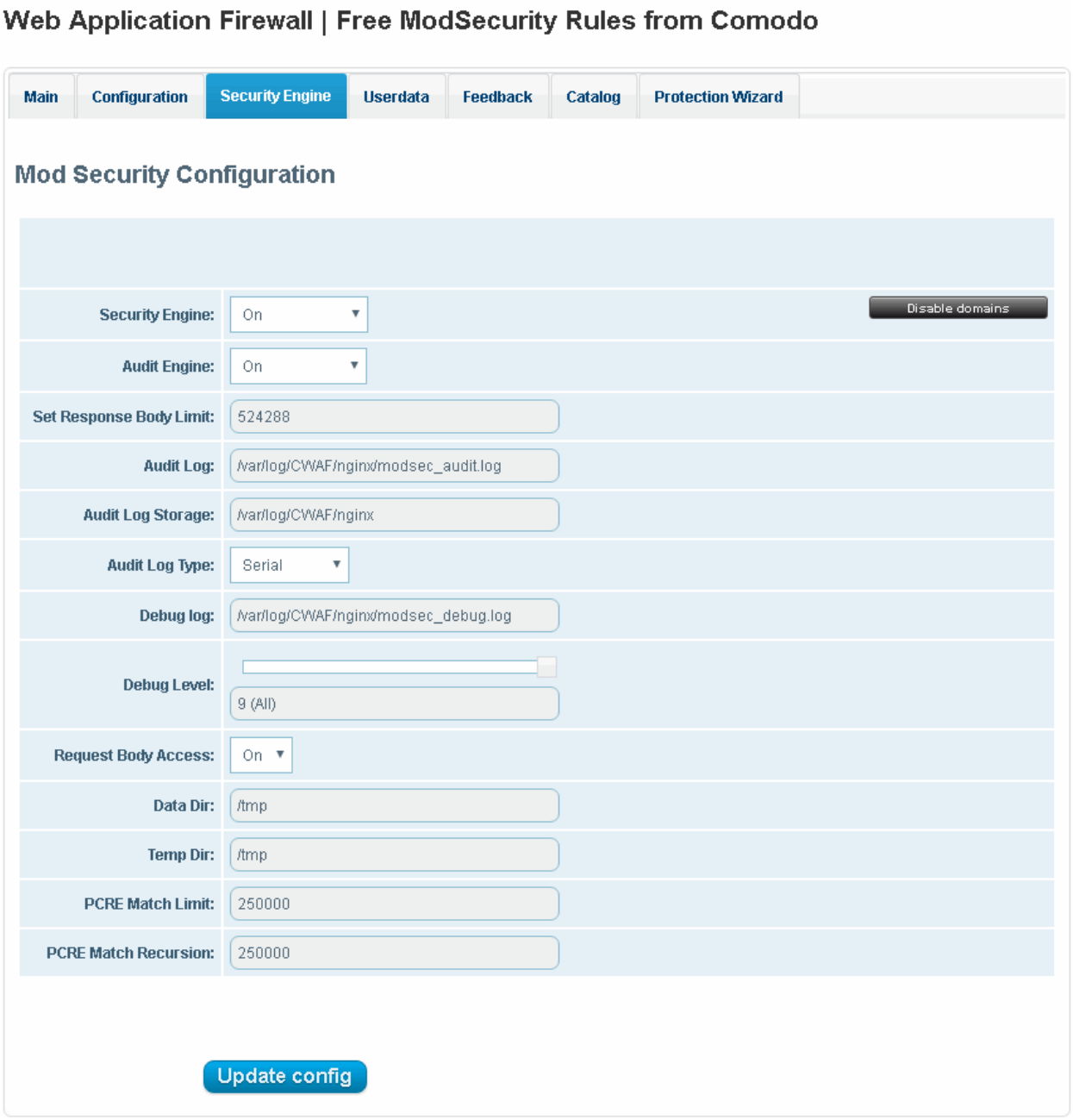
- Click the 'Update config' button to save your changes.



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

2.4.3. Manage Security Engine

- The 'Security Engine' tab lets you configure various settings related to your mod_security rules
- You can also disable mod_security on certain domains



Mod Security Configuration

- **Security Engine**
  - On - Rules are active on the domain
  - Off - Rules are turned off on the domain
  - Detect Only - Rules will identify attacks but won't execute any actions (block, deny, drop, allow, proxy and redirect)
- **Audit Engine** - Configure the behavior of the audit logging engine. (***Default: Relevant Only).*** Available options:
  - On - Activates audit logging for all transactions
  - Off - Deactivates audit logging for all transactions
  - Relevant Only - Logs transactions that have triggered a warning, error, or have a status code that is considered to be relevant.
- **Set Response Body Limit** – Set the max. size of response body in bytes. This is useful to optimize the

time that the web server waits to post a HTTP response.

When the response limit are over the specified size it will be rejected with status code 500 (Internal Server Error). ***(Default: limit = 524288 (512 KB). Max limit =1 GB)***

- **Audit Log** - You can modify the path to the main audit log file ***(Default: /usr/local/apache/logs/modsec_audit.log)***
- **Audit Log Storage -** You can modify the path to the audit log storage directory ***(Default: /usr/local/apache/logs/modsec_audit)***
- **Debug log** - You can modify the path to the debug log file ***(Default: usr/local/apache/logs/modsec_debug.log***)
- **Debug Level** - Set the level of logging the CWAF events. (***Default: 0***). The following table shows the list of levels:

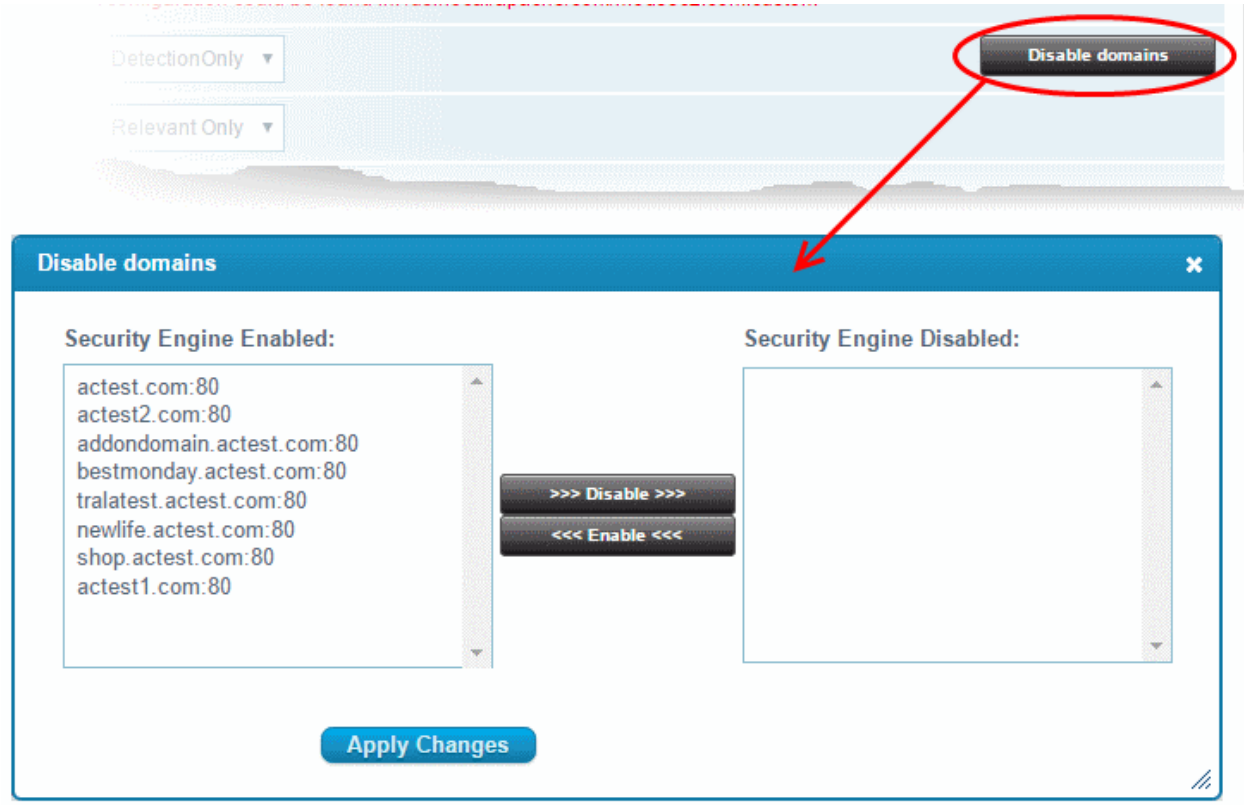
Level	Description
0	No events will be logged.
1	All errors (intercepted requests) will be logged.
2	All Warnings will be logged.
3	All Notifications will be logged.
4	Details of how transactions are handled will be logged.
5	As above but including information about each piece of information handled.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

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

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

The 'Disable domains' interface will display:



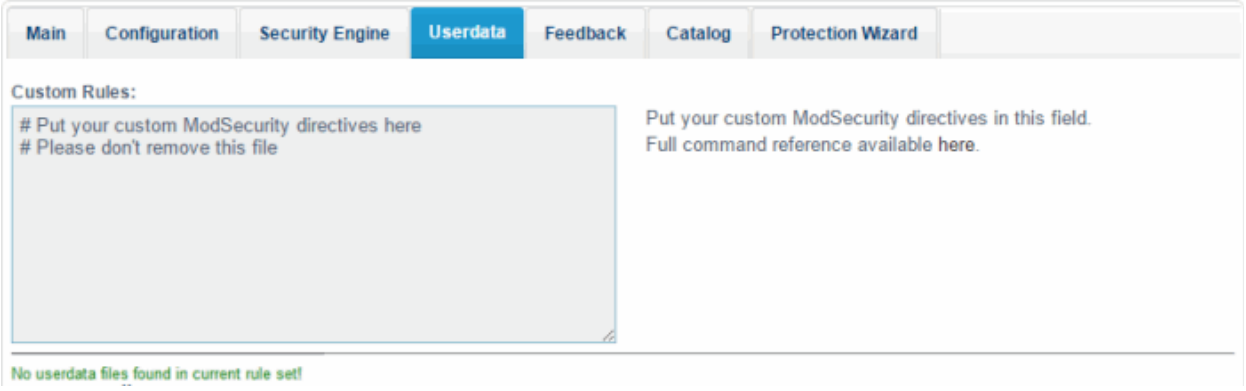
- Click on the domain or domains you wish to disable and click the '>>>Disable>>>' button to move it to the 'Disabled' list
- Click "Apply Changes" to save your configuration

- 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 lets you create custom rules.

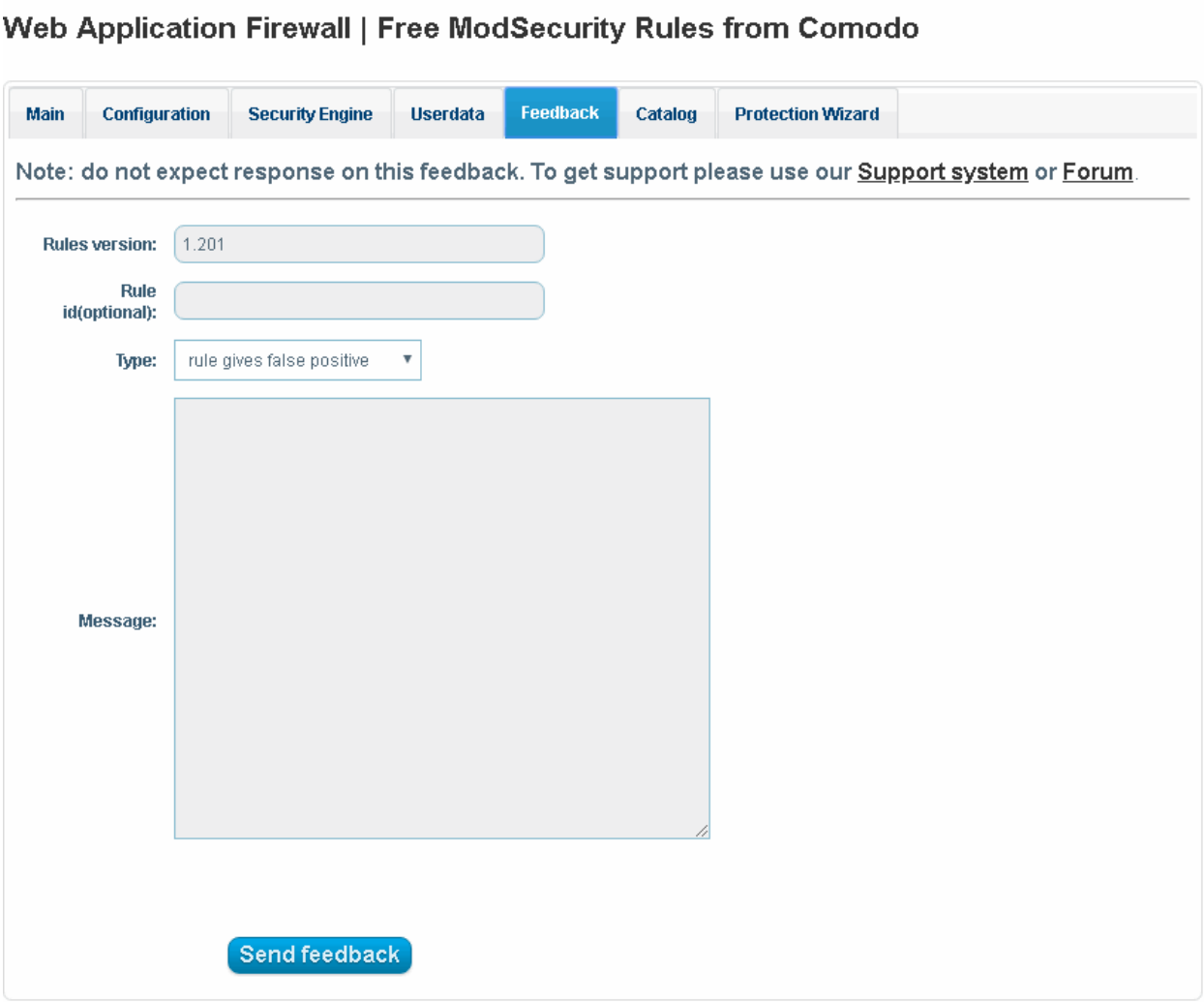


To add custom user rules settings, download the latest rule set version. See **View and Update CWAF Information** for more details.


Main
Configuration
Security Engine
Userdata
Feedback
Catalog
Protection Wizard
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.
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/
/if/
Put your restricted request headers here (one header per line).
By default any request headers are allowed.
If your want to block some request header then you should blacklist it here.
Save

2.4.5. Send Feedback

The feedback tab lets you send comments and suggestion on the currently loaded rule set to Comodo. Our technicians will consider all suggestions and may use them to enhance the rule set for the next version.



- **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

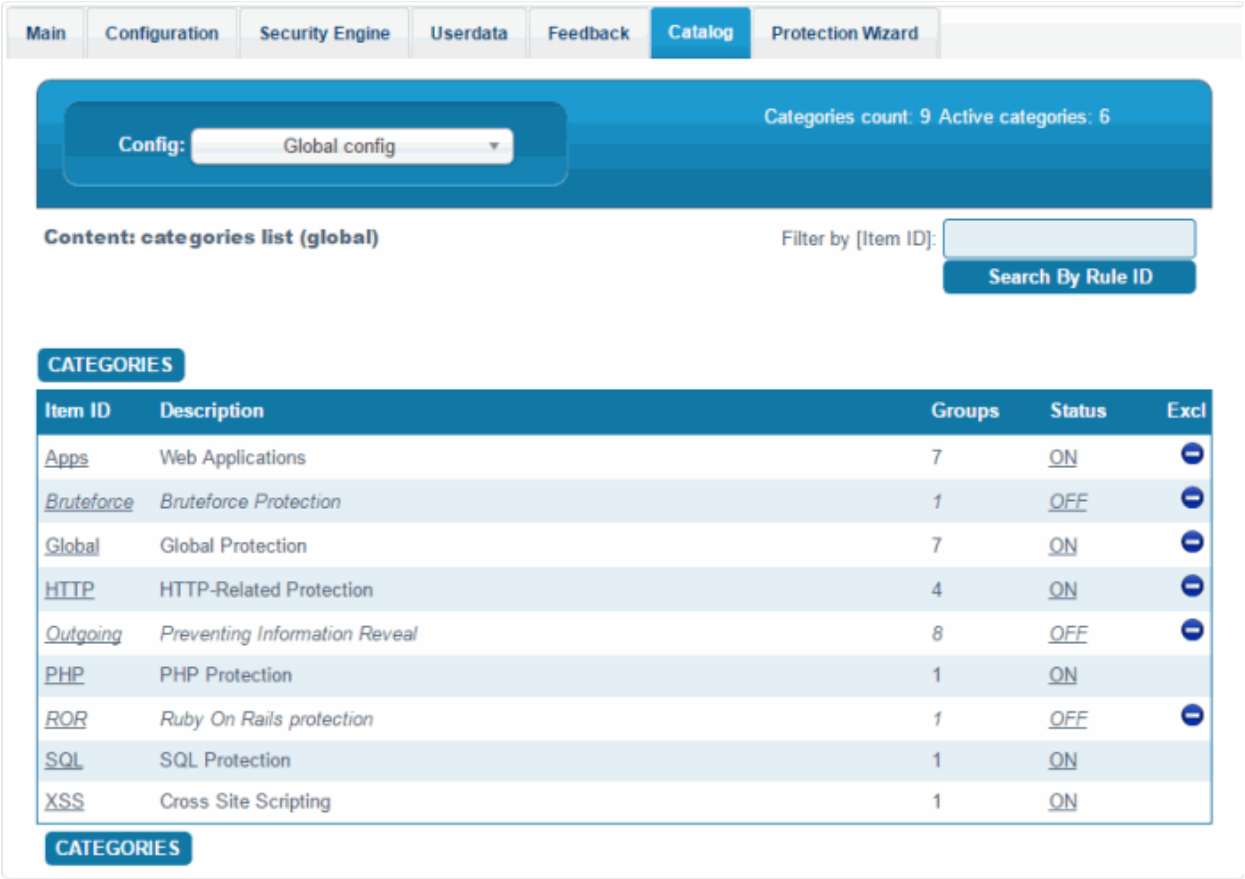
- Click 'Send feedback' to submit your feedback to Comodo

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

Note: DirectAdmin users - The **Feedback** feature is only available if you have provided credentials in the '**Configuration**' section.

2.4.6. Manage Catalog

- The catalog tab lets you specify rules that should be excluded from the currently loaded rule set
- By default the catalog is empty
- The list of domains appears only after a rule set has been downloaded
  - See **View and Update CWAF Information** if you need help to do this.



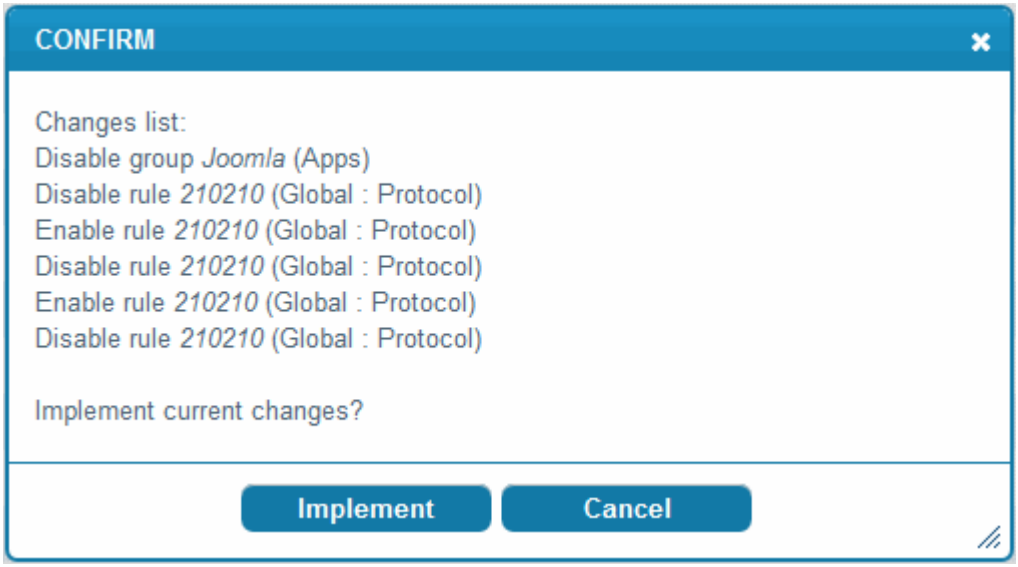
- **Config** - The scope of the operation. You can configure rules for the entire server or per-domain.
  - The catalog can be managed on three levels: categories, groups and rules.
  - Click the links in the 'Item ID' column to navigate between levels

Categories - Column Descriptions	
Column Heading	**Description**
Item ID	Variable field. Depending on the level, this field may contain: • A category name • A group name • A rule ID number Click the link in this column to move between levels.
Description	Brief information about the category, group or rule.
Groups	The number of groups in the current category
Status	States whether the rules in this category are enabled or disabled. • Click this link to enable or disable

Excl		Shows 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	Lets you move one level up/down in catalog hierarchy.

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

- Block an item in the 'GROUPS' level, to block all rule defined in that group.
- Block an item at the 'RULES' level, to 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.

Filter 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

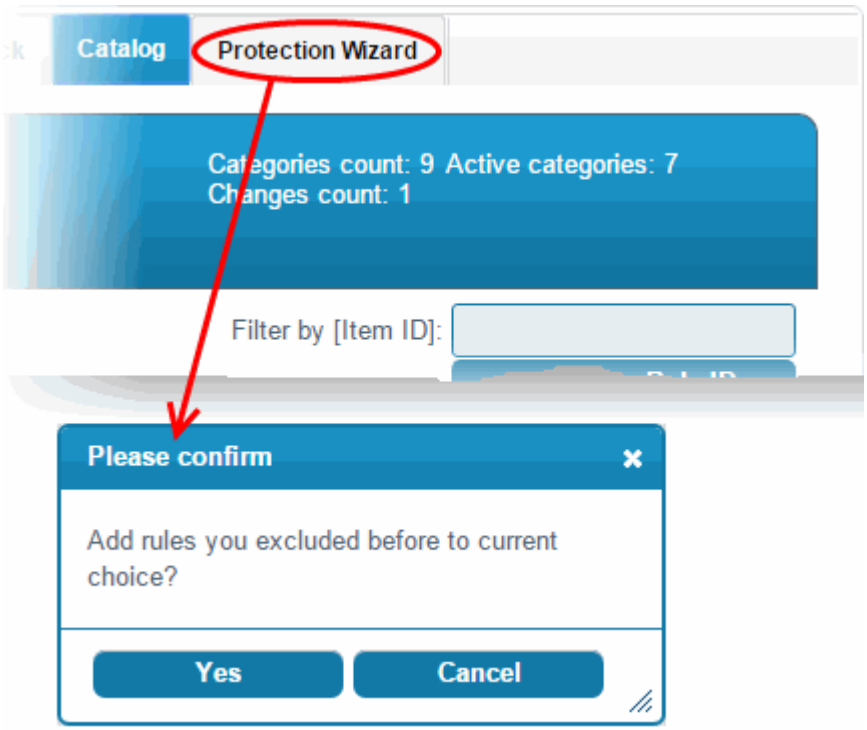
2.4.7. Protection Wizard

- The protection wizard tab lets you disable rules affecting web applications that are not installed on your

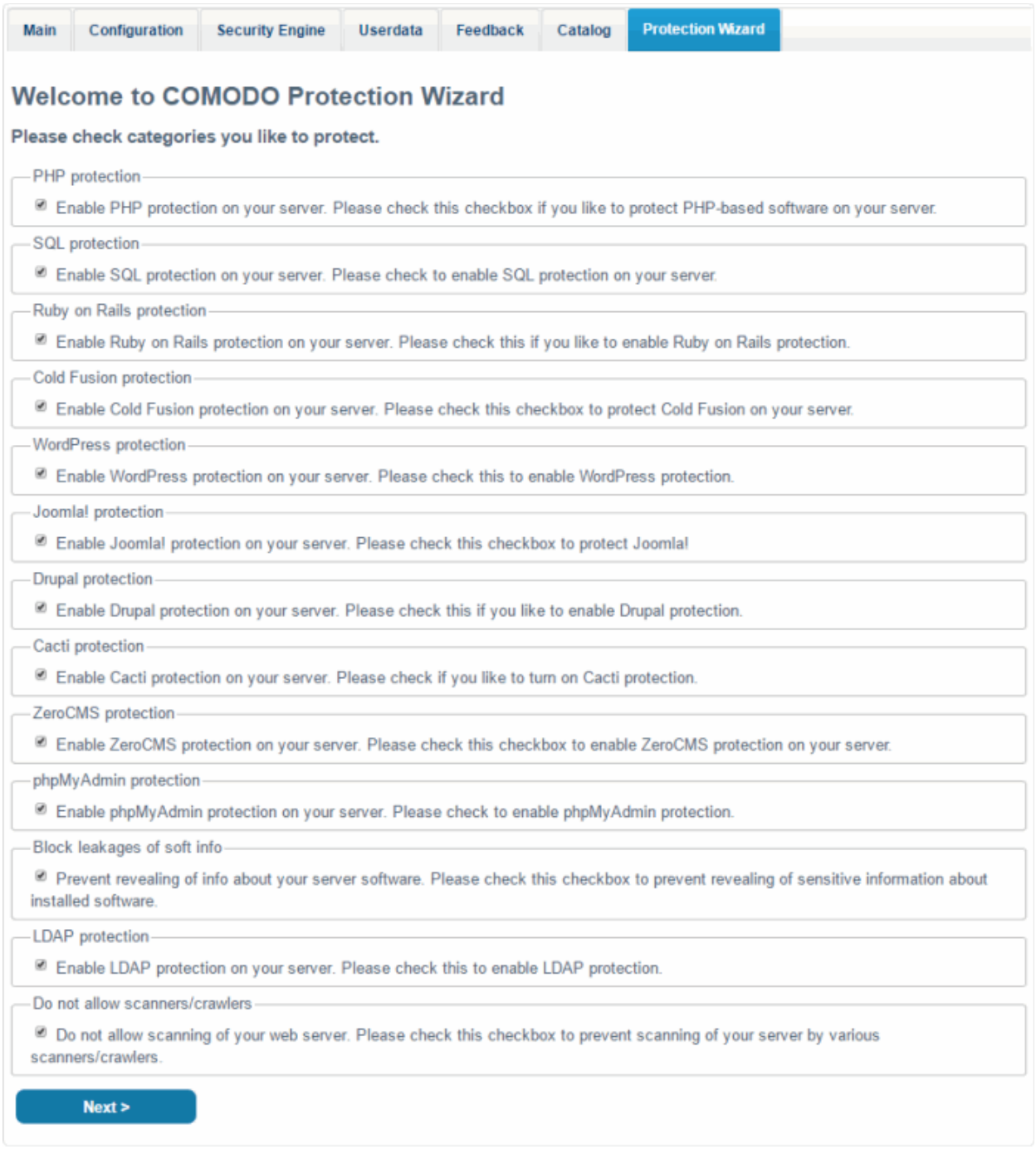
server. This helps to reduce server load.

- Though the functionality of this section is similar to the '**Catalog**' tab, the protection wizard is faster way to view all categories, groups and rules. This allows you to create rules for on installed applications.
- Previously excluded rules for a particular category can also be imported here and added to the global exclude list.

Open the protection wizard to add excluded rules back into your configuration. See the '**Catalog**' section for help configure the rule.

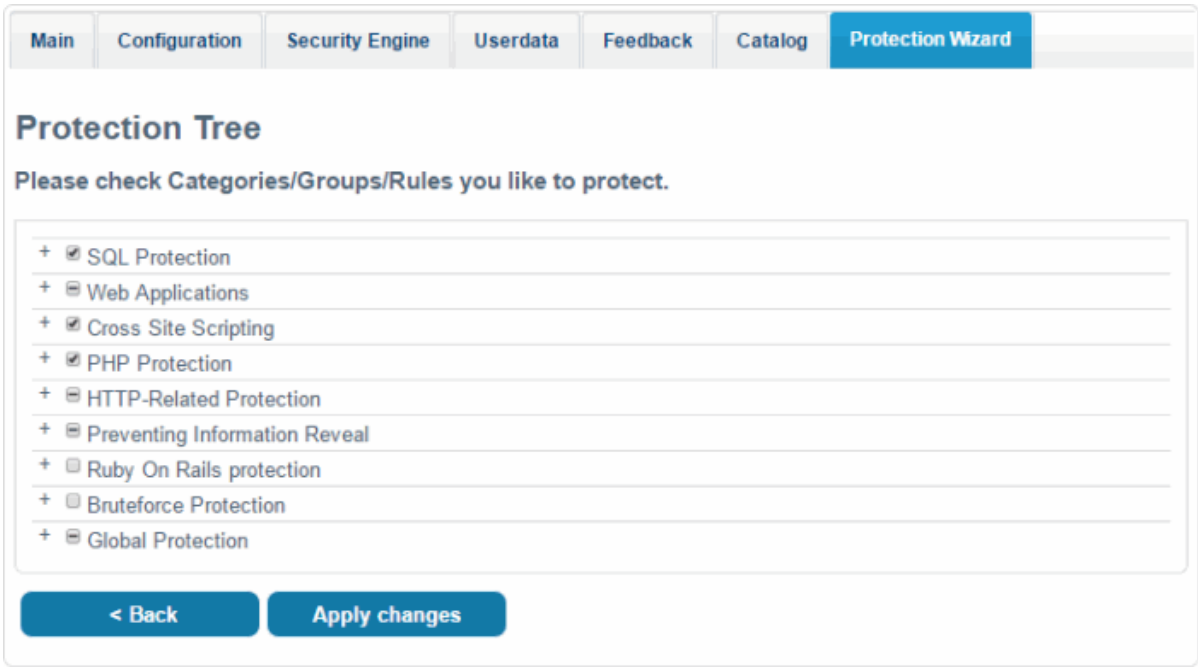


- Click 'Yes' to confirm the reinstatement
- Click 'Cancel' to review the full list and select the rules you want to enable

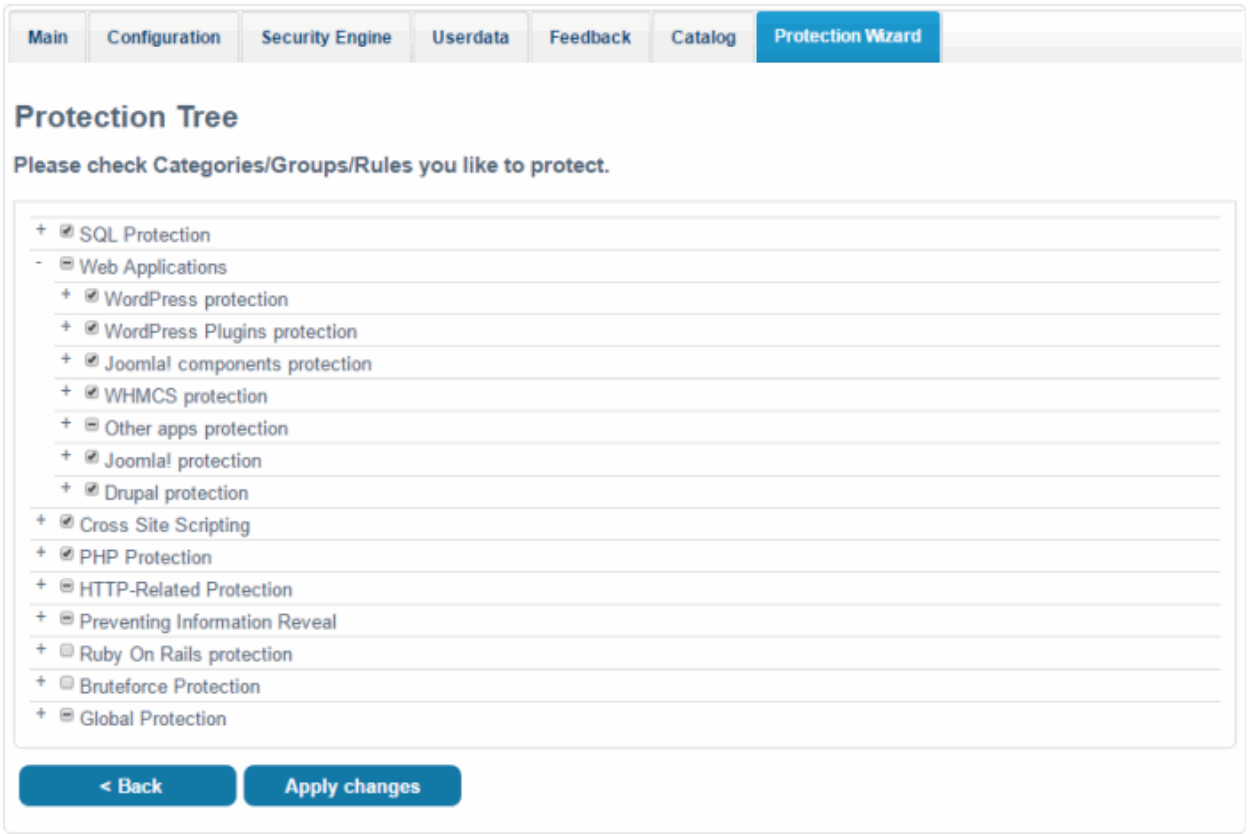


By default, all categories are enabled.

- You can enable/disable categories as required.
- Click the 'Next' button to open 'Categories', 'Groups' and 'Rules' in a tree structure.



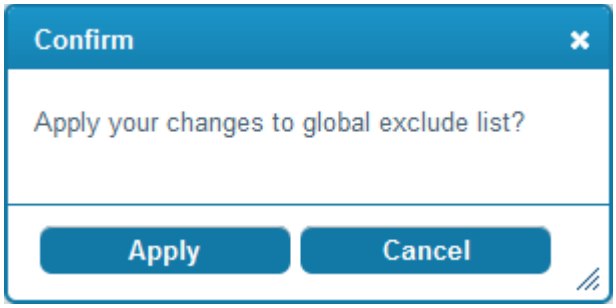
- Click the expand/collapse button ▸ beside a category/group/rule to enable or disable



Excluded rules are deselected in the list if you chose 'Yes' when opening the protection wizard.

- Enable or disable items as required then click 'Apply changes'.

A confirmation dialog appears:



- Click' Apply' in the confirmation box to implement your choices to the global exclude list.

2.5. Use the Agent for Firewall Configuration

The agent allows Linux admins to manually download and deploy the latest version of the Firewall Rule Sets.

Update the rule set to the latest version

- Run the CWAF console tool (assuming Agent was installed to /opt/cwaf):

/opt/cwaf/scripts/updater.pl

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

/var/log/CWAF/utils.log

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

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

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

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

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

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

The administrator can assign these scripts to be run periodically as Cron jobs. To get more information see “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. See 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 CWAF install tree
- Domain name should be specified as it looks in plugin or result of "--domain_list" command
- Use --force_domain to perform operations with domains not listed in --domain_list

2.7. Uninstall CWAF

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

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

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

Uninstall CWAF for cPanel

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

  You will be asked:

  Do you want to remove Comodo WAF application from cPanel?

  Enter answer [y/n] y

Uninstall CWAF for DirectAdmin

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

You will be asked:

Do you want to remove Comodo WAF application from DirectAdmin?

Enter answer [y/n] y

Uninstall CWAF for Plesk

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

  You will be asked:

  Do you want to remove Comodo WAF application from Plesk?

  Enter answer [y/n] y

Uninstall CWAF for Webmin

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

  You will be asked:

  Do you want to remove Comodo WAF application from Webmin?

  Enter answer [y/n] y

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:

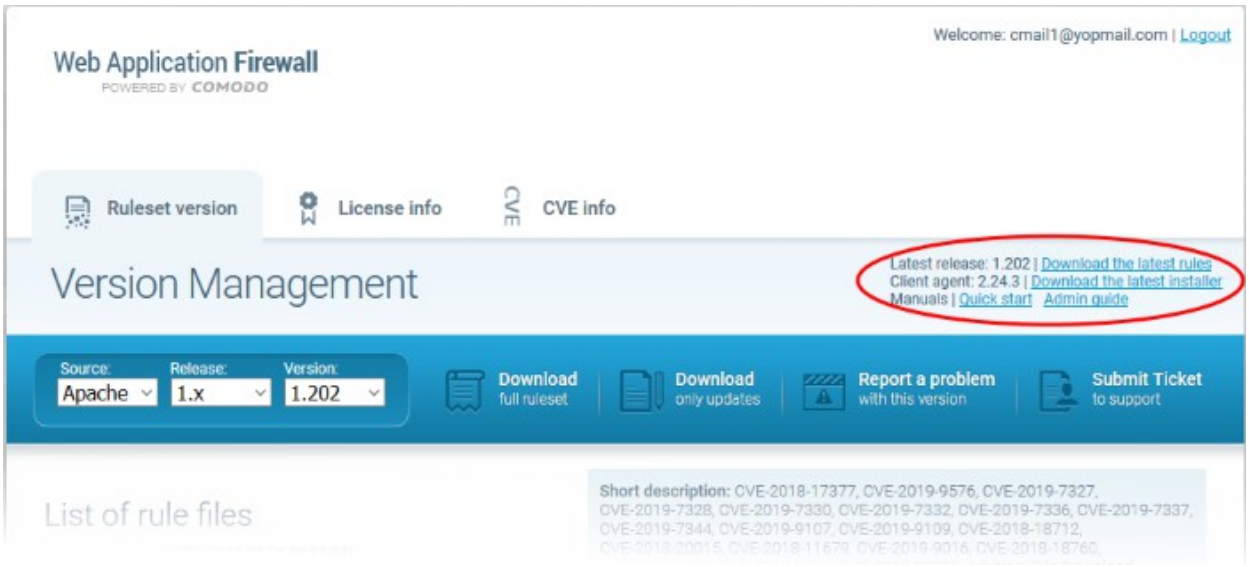
- Remove the string '*include /opt/cwaf/etc/cwaf.conf*' from the file '*/etc/apache2/conf/modsec2.conf*'
- Reload 'Apache'

The agent will be removed from the server.

2.8. Download and Install Rule Set Packages

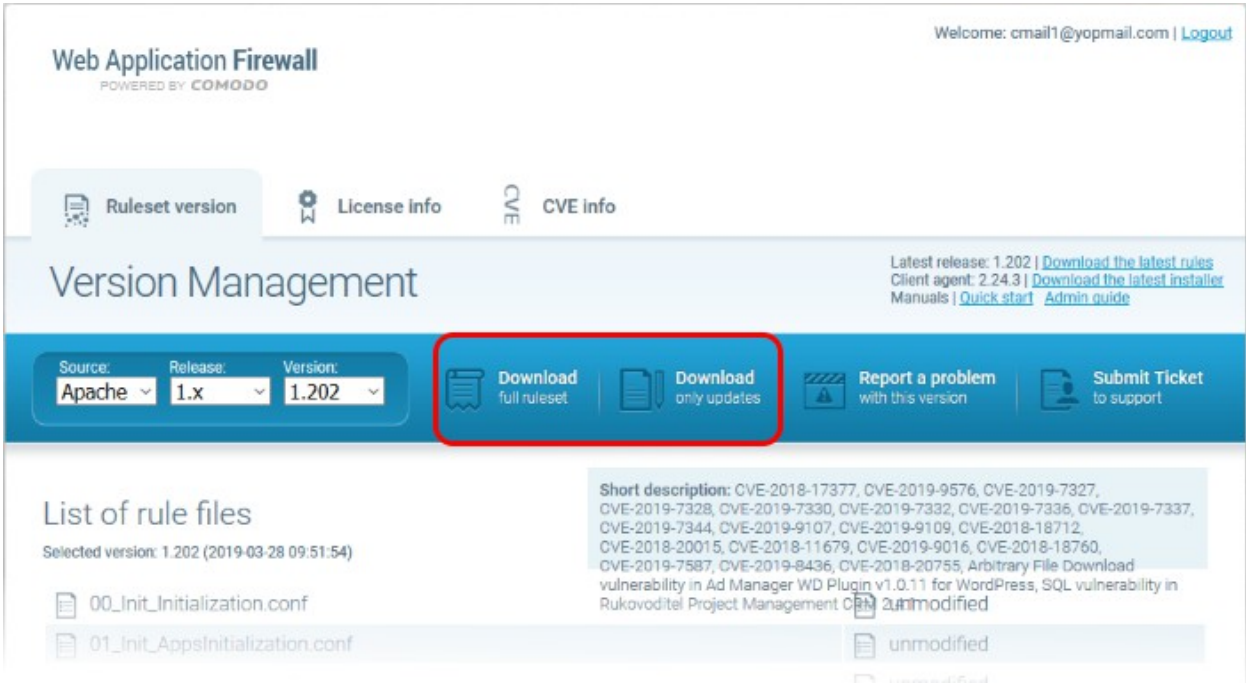
Download the Rule Set

- Log-in to the web admin console at **https://waf.comodo.com**
- 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 directly



- 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.



- 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.

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:, t*o include the following configuration key:

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

The rule sets in the package will be implemented immediately.

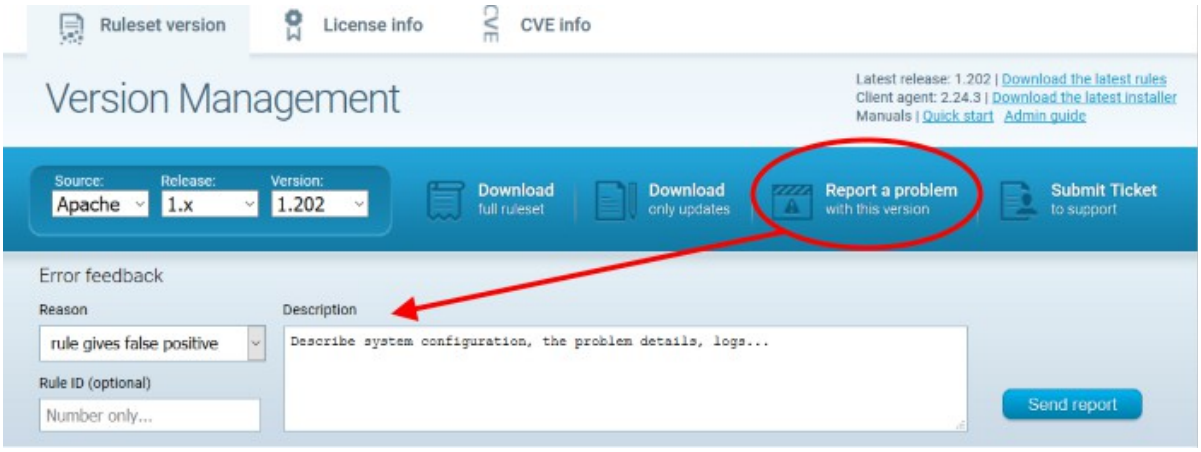
If you want to view or download the CWAF help guide, click the 'Manual' shortcut link at the top right.

2.9. Report Problems to Comodo

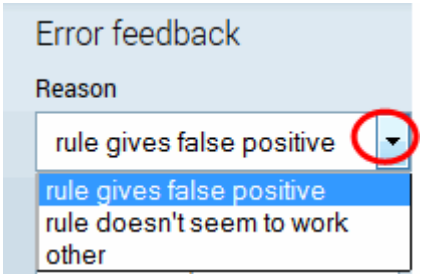
- Customer feedback plays a key role in developing and improving Comodo Web Application Firewall.
- The 'Report a problem' feature enables admins to post feedback and report problems on the currently loaded rule set and to notify us of any false positives.

Submit feedback

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



- **Reason** - Choose a subject for your feedback from the drop down menu.
- **Rule ID** - You can enter the ID number of the specific rule upon which feedback is provided. This field is optional.
- **Description** – Provide a brief information 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.

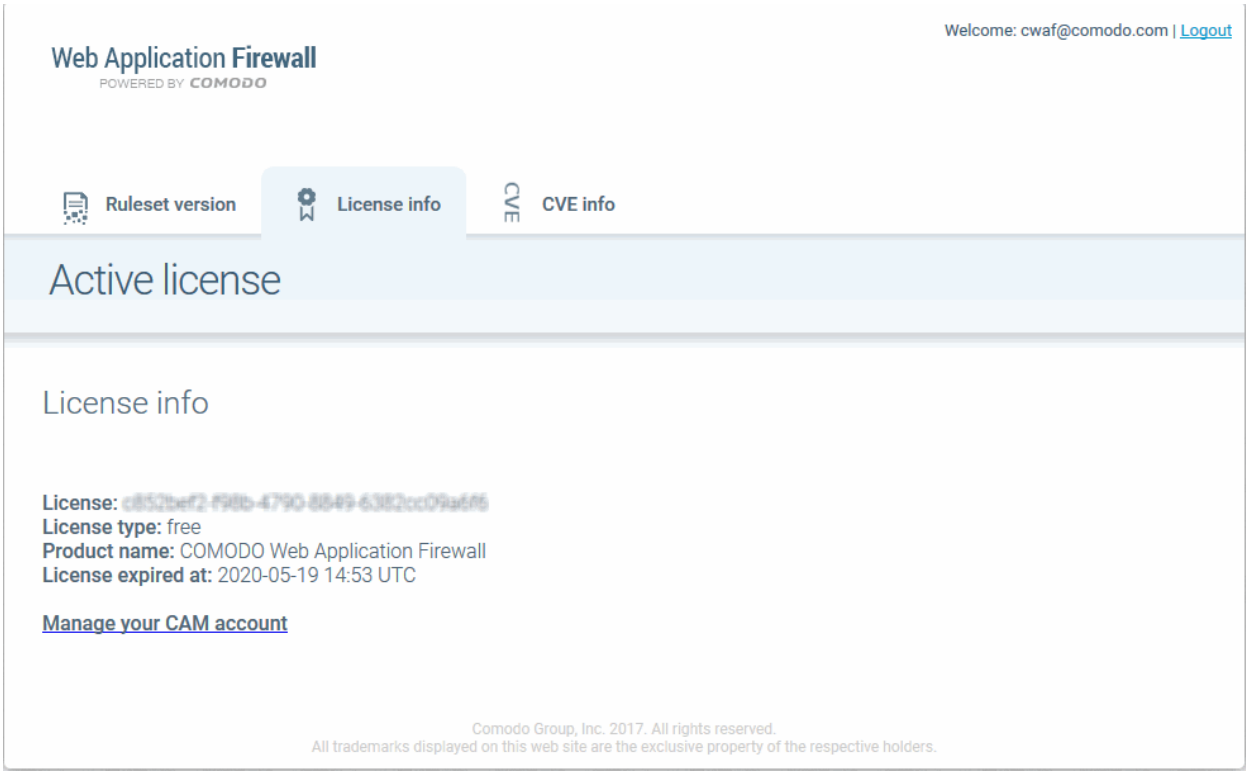
2.10. Submit Tickets to Comodo

Submit a support ticket

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

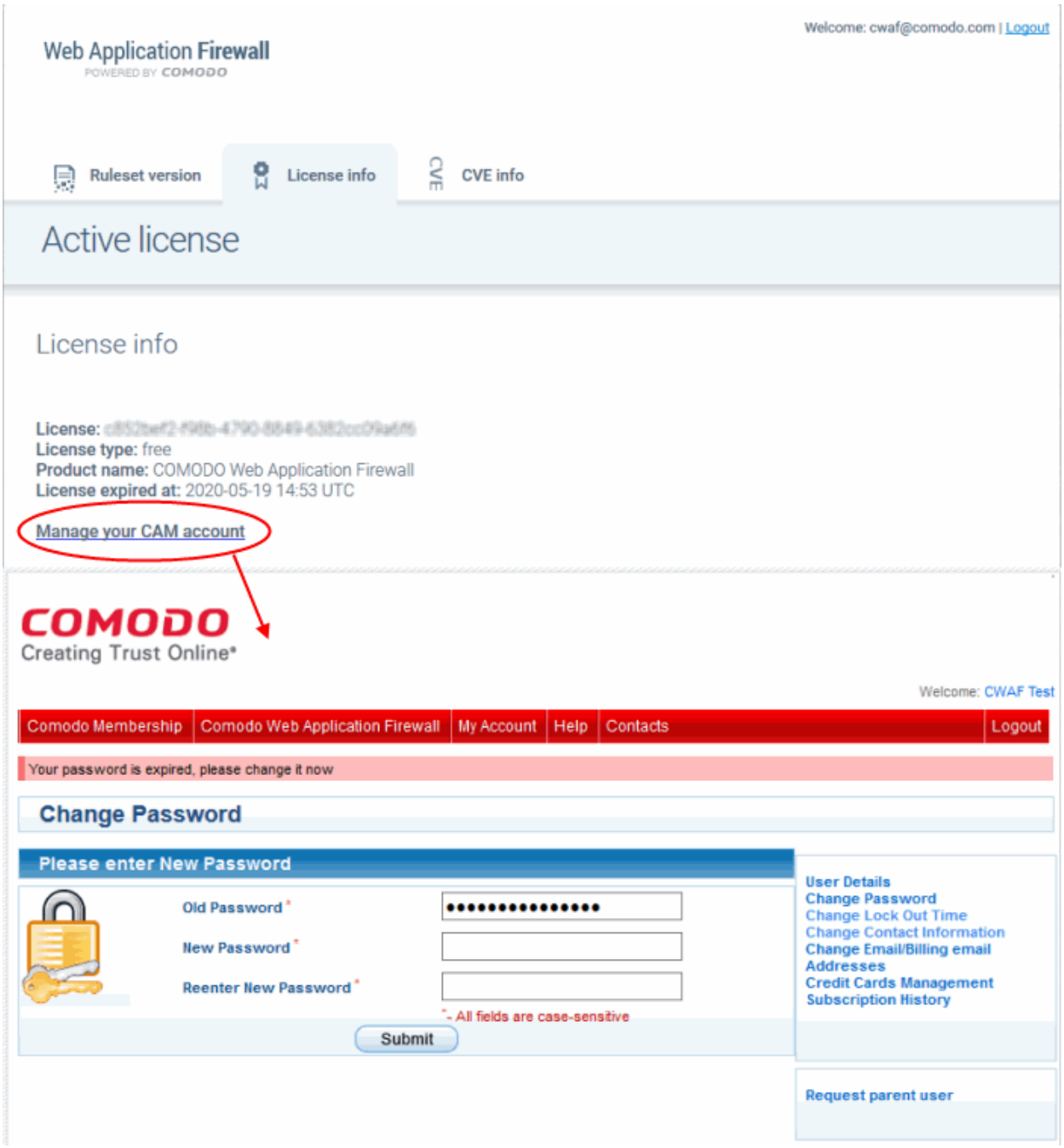
3. Manage CWAF License

- 'License Info' tab lets you view license information at the Comodo Account Management (CAM)
- The interface also provides a shortcut to login to your CAM account should you need to renew or upgrade your license



- **License** - The account authorization key.
- **License type:** The category of license - free or paid.
- **Product name** - The label of the product for which you have a license.
- **License expired at** - The expiration date of the license.
- **Manage your CAM account** - Navigates 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 see the Comodo Accounts Manager online help guide at **http://help.comodo.com/topic-211-1-513-5907—Introduction-To-Comodo-Accounts-Manager.html**.

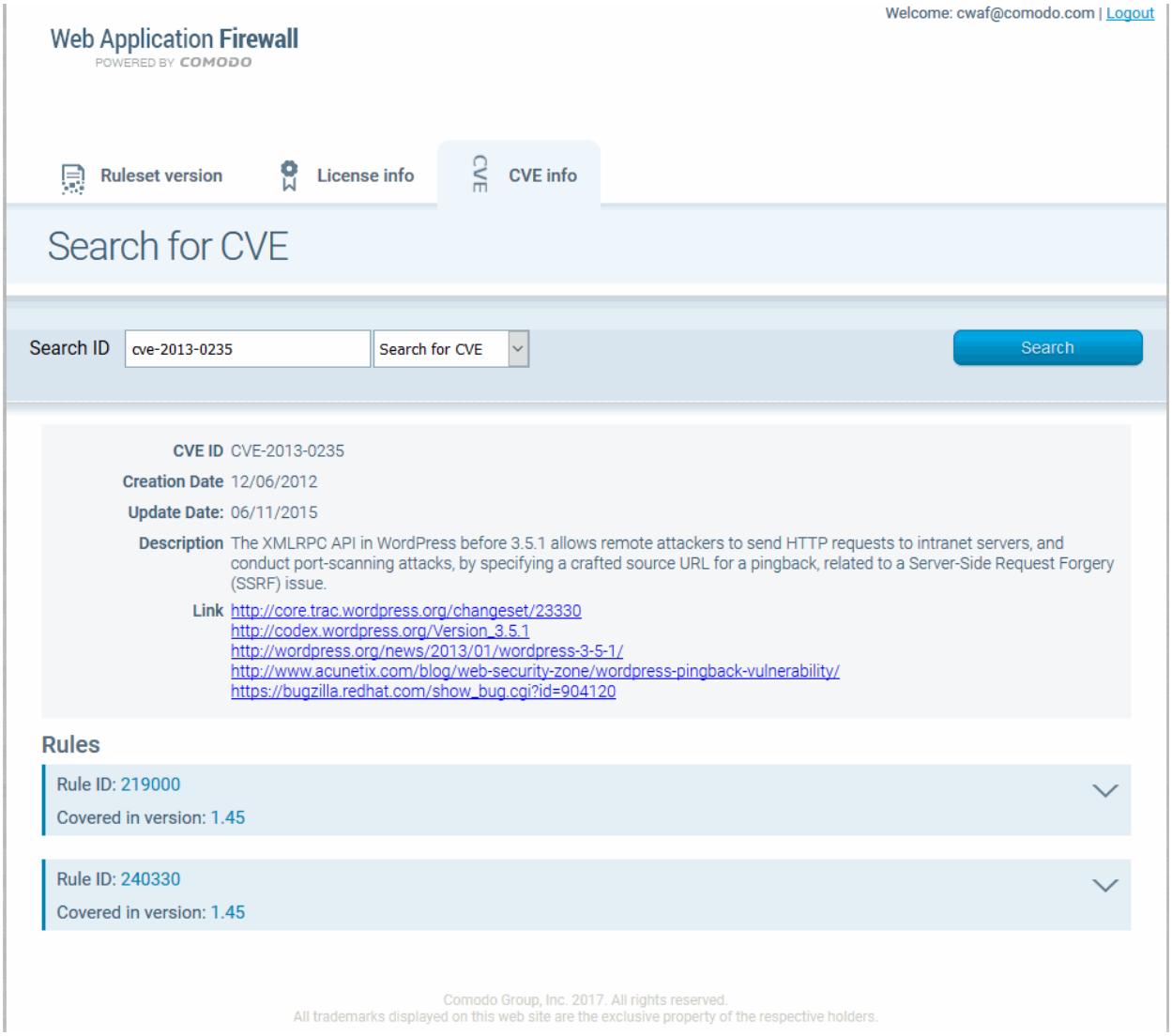


4. CVE Coverage Information

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



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 CWAF rules will be displayed.

Appendix 1 - Identify 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 **Use the Web Host Control Panel Plugin for Firewall Configuration** > '**Manage 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

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*'

Exclude a rule that is not needed (Plesk)

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

  Example:

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

  *SecRule REQUEST_HEADERS:Cookie "@rx (^|;)=(;|$)" *

  "id:220020,

  msg:'COMODO WAF: found CVE-2012-0021 attack',

  phase:1,

  deny,

  status:403,

log"

- Get the rule ID from the string.

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

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 **Use the Web Host Control Panel Plugin for Firewall Configuration** > **'Manage 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 or our **blog**. You can also follow us on **Twitter** (@ComodoDesktop) or **LinkedIn**.

1255 Broad Street

Clifton, NJ 07013

United States

Tel : +1.877.712.1309

Tel : +1.888.551.1531

https://www.comodo.com

Email: **EnterpriseSolutions@Comodo.com**