COMODO
Creating Trust Online®

Web Application Firewall
POWERED BY COMODO

Comodo
Web Application Firewall

Software Version 2.24

Quick Start Guide

Guide Version 2.24.010620

Comodo Security Solutions
1255 Broad Street
Clifton, NJ 07013

1. Comodo Web Application Firewall - Quick Start Guide

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

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

- **Step-1 - Sign-up for Comodo Web Application Firewall**
- **Step 2 - Login to admin console**
- **Step 3 - Download rule sets and deploy on to server by anyone of the following methods:**
    - **Use plugin for automatic download and deployment of rule set updates**
        - **Install the web hosting control panel plugin on Linux**
        - **Use CWAF Agent to download and deploy the Rule Sets on standalone mode**
        - **Install the Ruleset on Windows IIS**
    - **Download the rule sets from web admin console and install on to server**

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

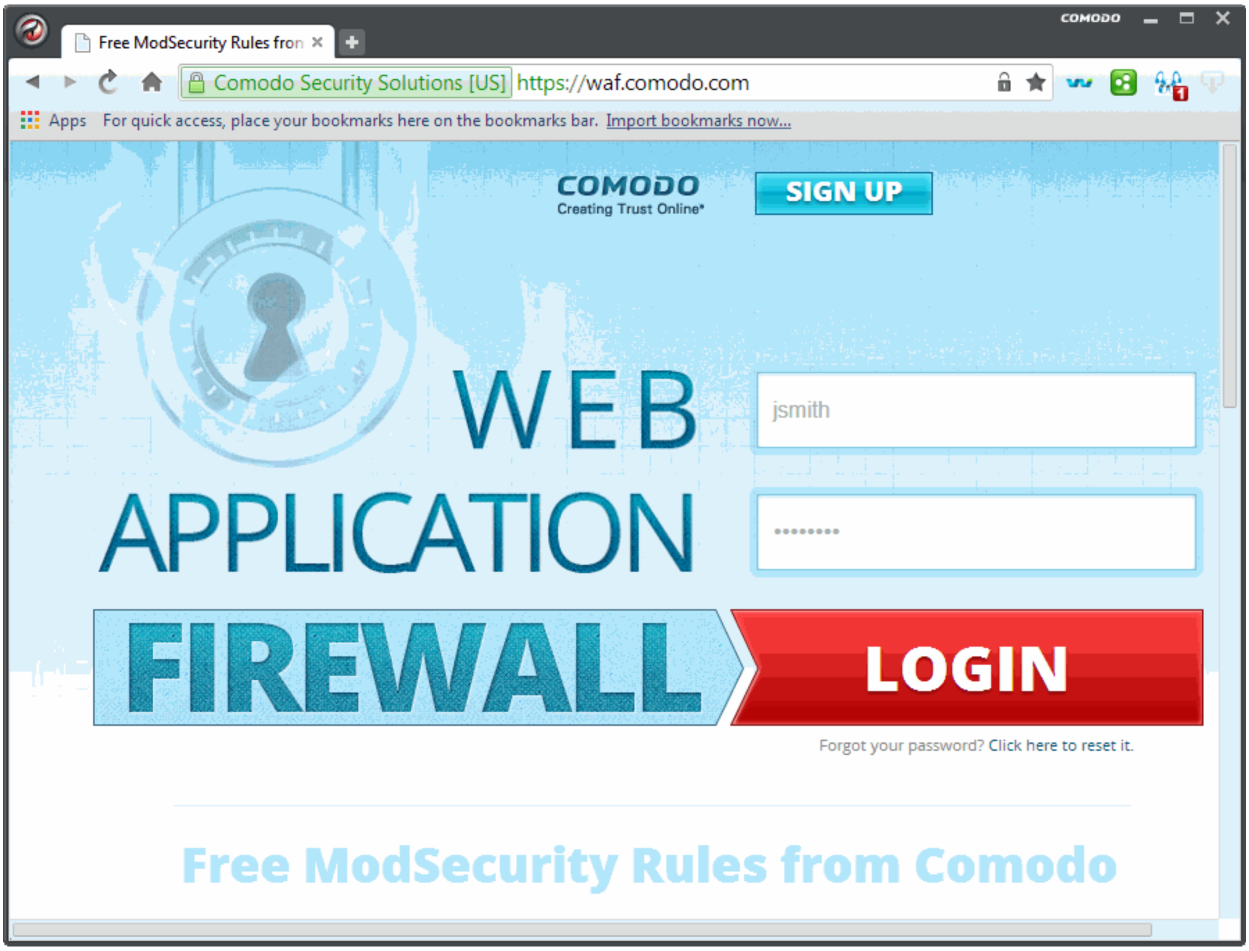
- Sign-up for the CWAF service from the Comodo Accounts Manager at **https://accounts.comodo.com/cwaf/management/signup**.
- Select the CWAF product from the list
- Fill-in your user details and billing information
- Select the payment mode and enter your payment details
- Read the 'End User License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

Upon successful payment processing, your account will be activated.

Sign-in to Comodo Web Application Firewall administration interface at **https://waf.comodo.com** with the same username and password you specified during signing up and manage your Web Application Firewall.

Step 2 - Login to Admin Console

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



Free ModSecurity Rules fron

Comodo Security Solutions [US] https://waf.comodo.com

Apps For quick access, place your bookmarks here on the bookmarks bar. Import bookmarks now...

COMODO Creating Trust Online*

SIGN UP

WEB APPLICATION FIREWALL

jsmith

••••••••

LOGIN

Forgot your password? Click here to reset it.

Free ModSecurity Rules from Comodo

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

You will be taken to the CWAF web admin console.

Step 3 - Download rule sets and deploy on to server

Comodo periodically publishes pre-defined firewall rule sets for the CWAF, which can be downloaded and deployed on to your web application server.

Follow one of the methods given below to download and deploy the rule sets, and to keep them up-to-date:

- **Use plugin for automatic download and deployment of rule set updates**
  - **Install the web host control panel plugin on Linux**
  - **Use CWAF Agent to download and deploy the Rule Sets on standalone mode**
  - **Install the Ruleset on Windows IIS**
- **Download the rule sets from web admin console and installing on to server**

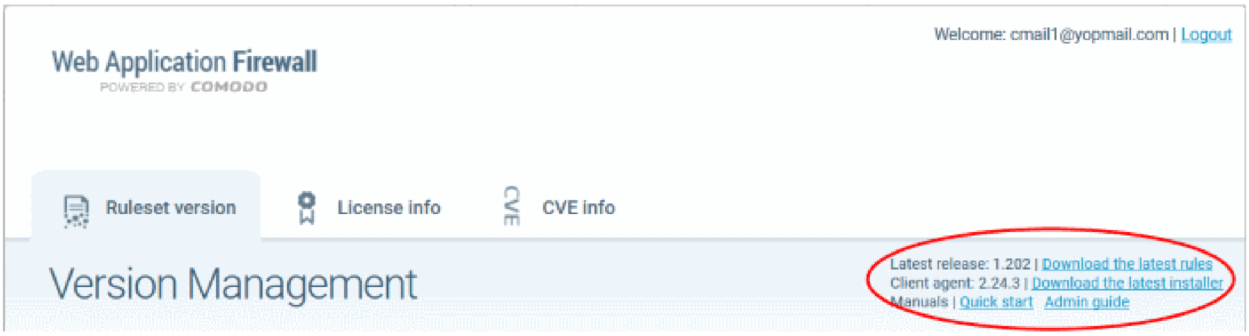
Use plugin for automatic download and deployment of rule set updates

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

Download the Agent

- Log-in to the web admin console at **https://waf.comodo.com**
- Open the 'Rule set version' tab

- Click the 'Download latest installer' link at the top-right


Web Application Firewall
POWERED BY COMODO
Welcome: cmail1@yopmail.com | Logout
Ruleset version
License info
CVE info
Version Management
Latest release: 1.202 | Download the latest rules
Client agent: 2.24.3 | Download the latest installer
Manuals | Quick start Admin guide

- Download and save the agent setup file.

Install the web host control panel plugin on Linux

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

  E.g. `/root`

- Run it installation script with a root privileges:

  # bash /root/cwaf_client_install.sh

Step 1

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

1) Check for Apache and its version:

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

Checking for mod_security and its version:

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

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

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

2) Check for LiteSpeed and LiteSpeed mod_security:

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

3) Check for Nginx:

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

4) Checking for prerequisites:

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

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

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

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

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

Update mode).

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

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

6) Check for required Perl modules:

CWAF will check for Perl modules and install them if required

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

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

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

Step 2

Select the web platform:

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

Step 3

Enter login credentials for Comodo Web Application Firewall.

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

Use CWAF Agent to download and deploy the Rule Sets on standalone mode

Install the agent on to the server

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

  E.g. `/root`

- Run it installation script with a root privileges:

  # bash /root/cwaf_client_install.sh

The Installation steps for the standalone mode are the same as for the plug-in. See **Install the Web Host Control Panel Plugin** for more details.

Step 4

Required for installation in standalone mode

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

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

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

and reload Apache

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

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

Install the Ruleset on Windows IIS

Please ensure you are running the following:

- IIS v 7.5
- Mod_security v 2.7.5 and above

To install Mod_security

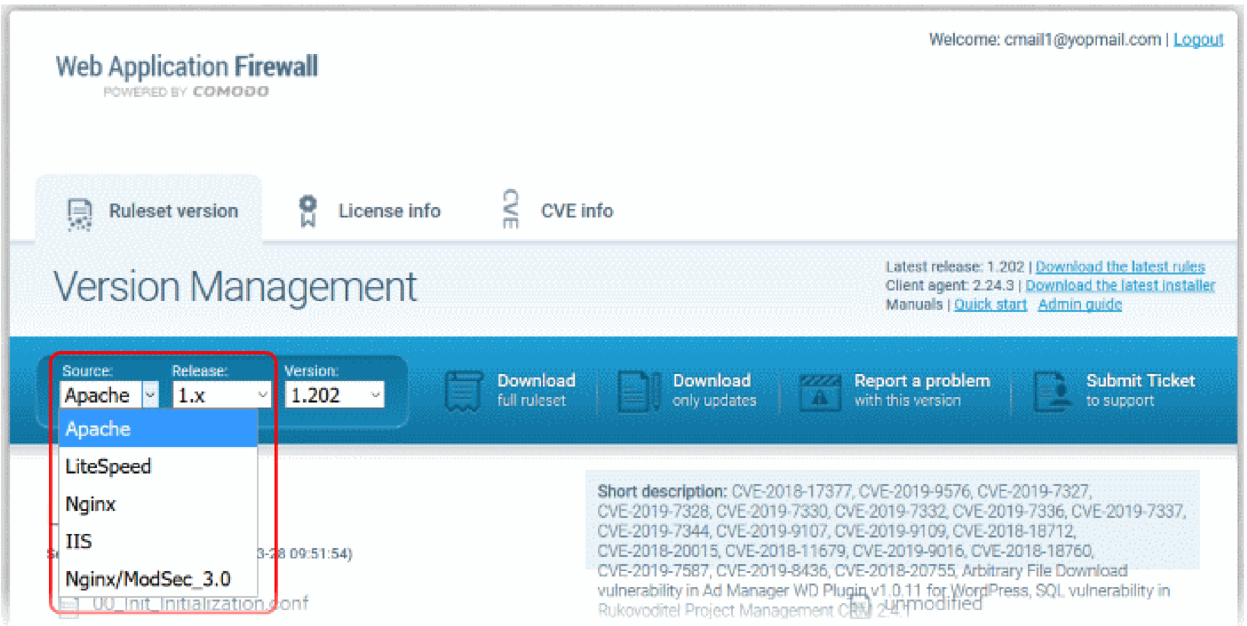
- Download and run **Mod_security installer**

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

<ModSecurity enabled="true" configFile="c:pathtocwafmodsecurity_iis.conf" />

Download and install CWAF rules

- Log-in to the web administration console at **https://waf.comodo.com/**
- Ensure that the 'Rule set version' tab is open
- Select 'IIS' from the 'Source' drop-down
- The rule sets contained in the selected version of the package is listed under 'List of rule files' along with its release date and time



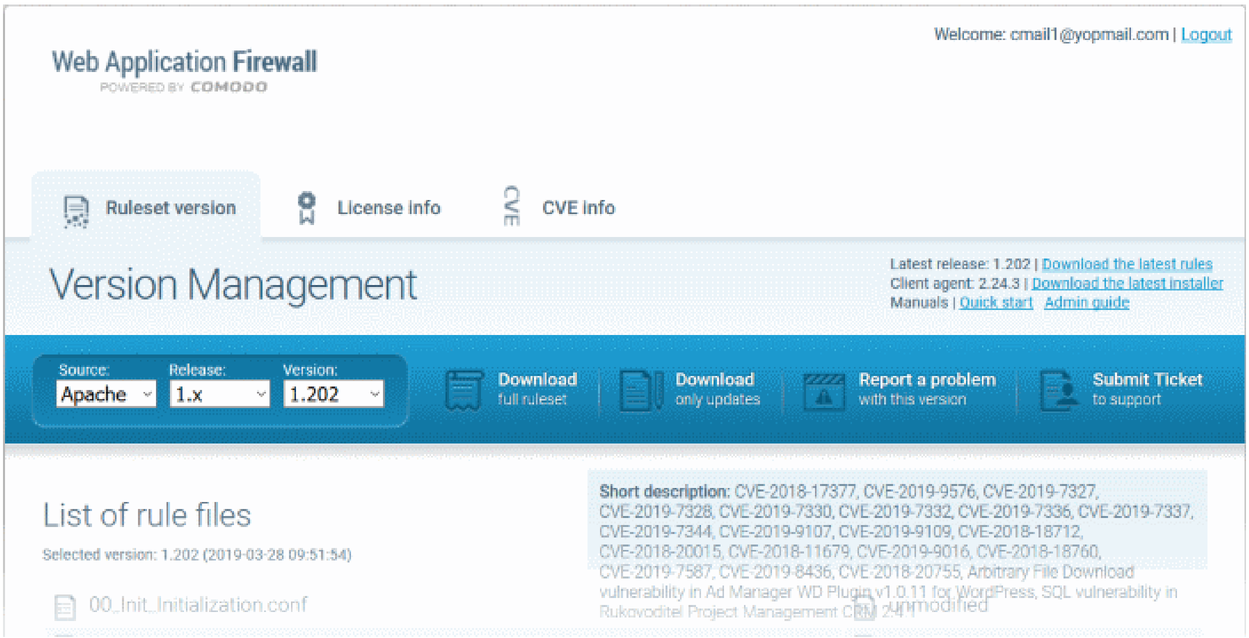
Welcome: cmail1@yopmail.com | Logout

Latest release: 1.202 | Download the latest rules
Client agent: 2.24.3 | Download the latest installer
Manuals | Quick start Admin guide

Source: Apache
Release: 1.x
Version: 1.202

Short description: CVE-2018-17377, CVE-2019-9576, CVE-2019-7327, CVE-2019-7328, CVE-2019-7330, CVE-2019-7332, CVE-2019-7336, CVE-2019-7337, CVE-2019-7344, CVE-2019-9107, CVE-2019-9109, CVE-2018-18712, CVE-2018-20015, CVE-2018-11679, CVE-2019-9016, CVE-2018-18760, CVE-2019-7587, CVE-2019-8436, CVE-2018-20755, Arbitrary File Download vulnerability in Ad Manager WD Plugin v1.0.11 for WordPress, SQL vulnerability in Rukovoditel Project Management CRM 2.4.1

- Click the 'Download full ruleset'



Welcome: cmail1@yopmail.com | Logout

Web Application Firewall
POWERED BY COMODO

Version Management

Latest release: 1.202 | Download the latest rules
Client agent: 2.24.3 | Download the latest installer
Manuals | Quick start Admin guide

Source: Apache
Release: 1.x
Version: 1.202

List of rule files

Selected version: 1.202 (2019-03-28 09:51:54)

00_Init_Initialization.conf

unmodified

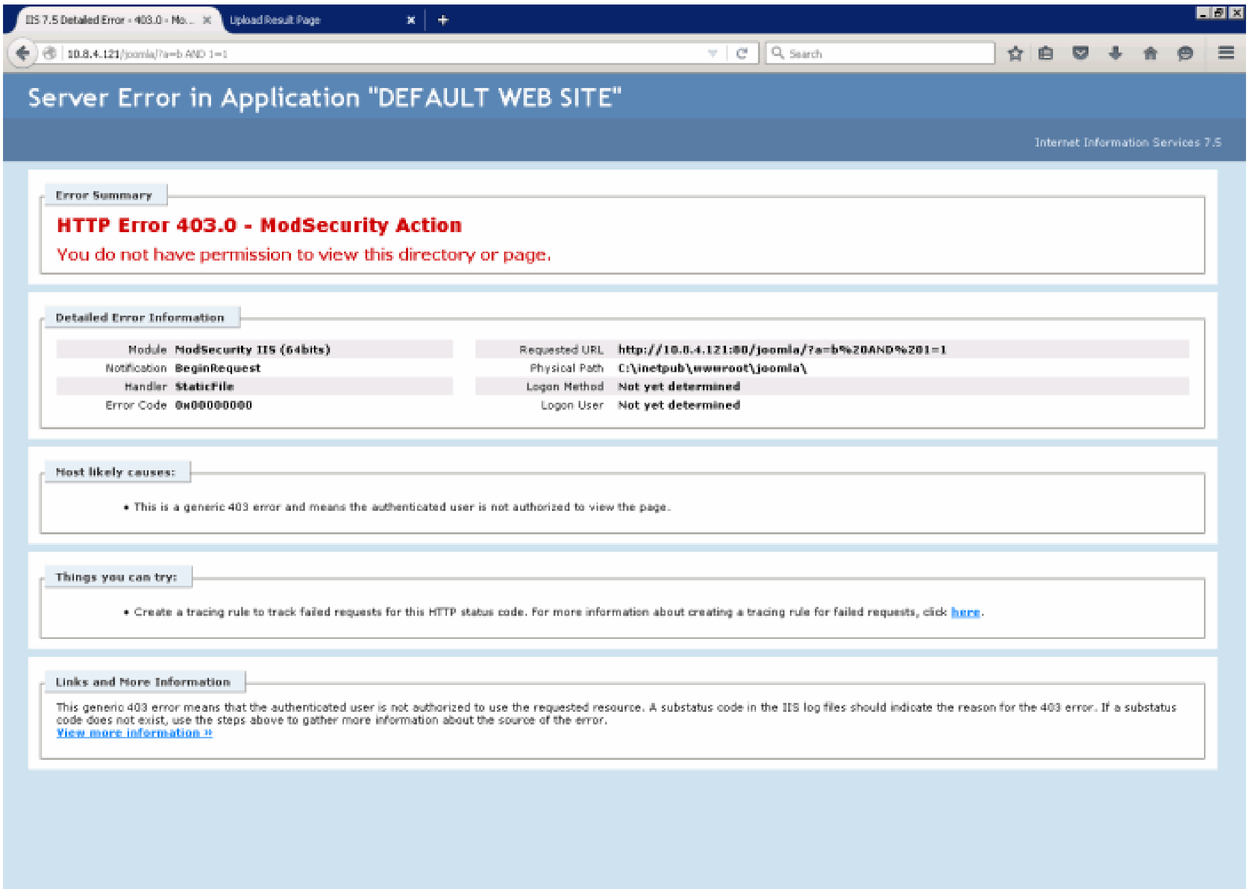
Short description: CVE-2018-17377, CVE-2019-9576, CVE-2019-7327, CVE-2019-7328, CVE-2019-7330, CVE-2019-7332, CVE-2019-7336, CVE-2019-7337, CVE-2019-7344, CVE-2019-9107, CVE-2019-9109, CVE-2018-18712, CVE-2018-20015, CVE-2018-11679, CVE-2019-9016, CVE-2018-18760, CVE-2019-7587, CVE-2019-8436, CVE-2018-20755, Arbitrary File Download vulnerability in Ad Manager WD Plugin v1.0.11 for WordPress, SQL vulnerability in Rukovoditel Project Management CRM 2.4.1

- Navigate to “C:\Program Files\ModSecurity IIS” folder 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 is shown:



IIS 7.5 Detailed Error - 403.0 - Mo...
Upload Result Page
10.8.4.121/joomla/?a=b AND 1=1
Search

Server Error in Application "DEFAULT WEB SITE"

Internet Information Services 7.5

Error Summary

HTTP Error 403.0 - ModSecurity Action

You do not have permission to view this directory or page.

Detailed Error Information

Module	**ModSecurity IIS (64bits)**	Requested URL	**http://10.0.4.121:80/joomla/?a=b%20AND%201=1**
Notification	**BeginRequest**	Physical Path	**C:\inetpub\wwwroot\joomla\**
Handler	**StaticFile**	Logon Method	**Not yet determined**
Error Code	**0x00000000**	Logon User	**Not yet determined**

Most likely causes:

- This is a generic 403 error and means the authenticated user is not authorized to view the page.

Things you can try:

- Create a tracing rule to track failed requests for this HTTP status code. For more information about creating a tracing rule for failed requests, click here.

Links and More Information

This generic 403 error means that the authenticated user is not authorized to use the requested resource. A substatus code in the IIS log files should indicate the reason for the 403 error. If a substatus code does not exist, use the steps above to gather more information about the source of the error.
View more information »

To run the protection rules updates

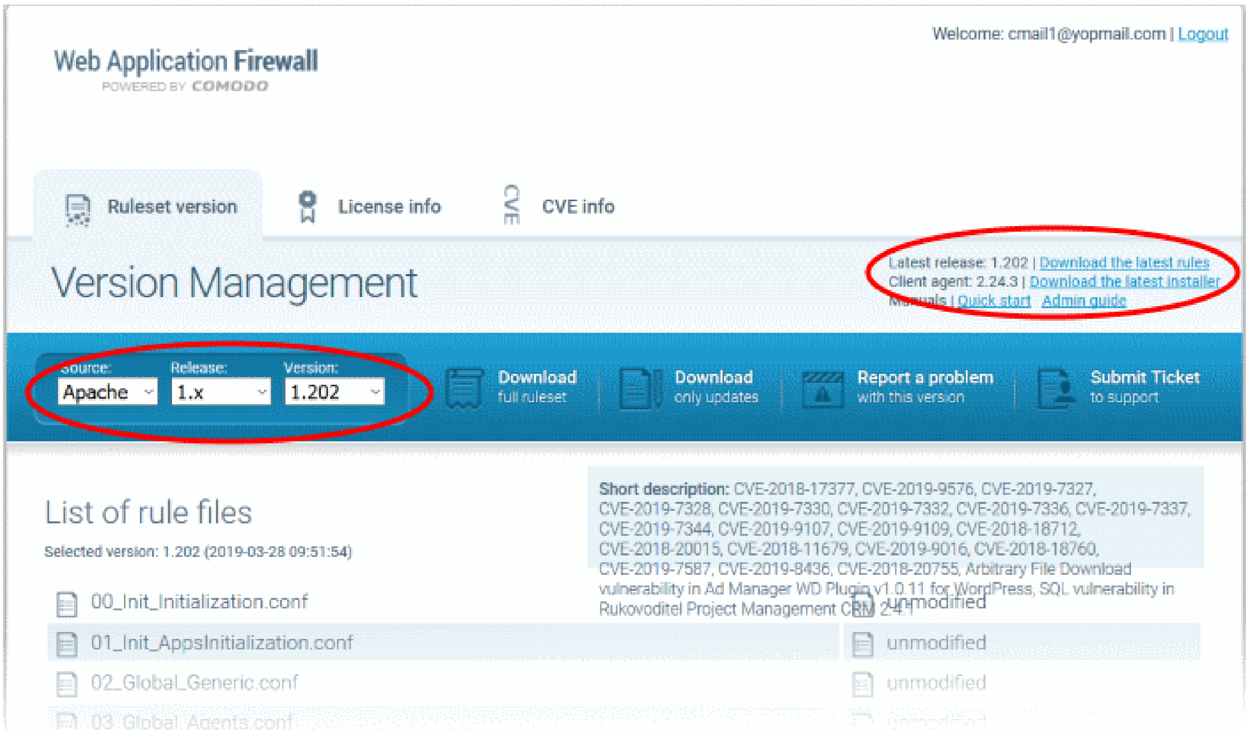
- Go to the 'Start' > 'Run' > cmd.exe to open a command prompt
- Run system command:

  cscript.exe "C:\Program Files\ModSecurity IIS\cwaf_update.vbs"

Download the rule sets from web admin console and install on to server

- Log-in to the web admin console at **https://waf.comodo.com**
- Open the 'Rule set version' tab
- Click the 'Download latest rules set' shortcut link at the top-right to download the latest version of the rules set package

  or
- Choose a source, version and release number from the drop-down to download the rules set package



Welcome: cmail1@yopmail.com | Logout

Version Management

Latest release: 1.202 | Download the latest rules
Client agent: 2.24.3 | Download the latest installer
Manuals | Quick start Admin guide

Source: Apache
Release: 1.x
Version: 1.202

List of rule files

Selected version: 1.202 (2019-03-28 09:51:54)

Short description: CVE-2018-17377, CVE-2019-9576, CVE-2019-7327, CVE-2019-7328, CVE-2019-7330, CVE-2019-7332, CVE-2019-7336, CVE-2019-7337, CVE-2019-7344, CVE-2019-9107, CVE-2019-9109, CVE-2018-18712, CVE-2018-20015, CVE-2018-11679, CVE-2019-9016, CVE-2018-18760, CVE-2019-7587, CVE-2019-8436, CVE-2018-20755, Arbitrary File Download vulnerability in Ad Manager WD Plugin v1.0.11 for WordPress, SQL vulnerability in Rukovoditel Project Management CRM 2.4.1

00_Init_Initialization.conf	unmodified
01_Init_AppsInitialization.conf	unmodified
02_Global_Generic.conf	unmodified
03_Global_Agents.conf	unmodified

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

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

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

The rule sets in the package will be implemented immediately.

- See the online help page **Download and install rule set packages** of the **Deploy CWAF Rules On Server** for more details on using the web admin console.

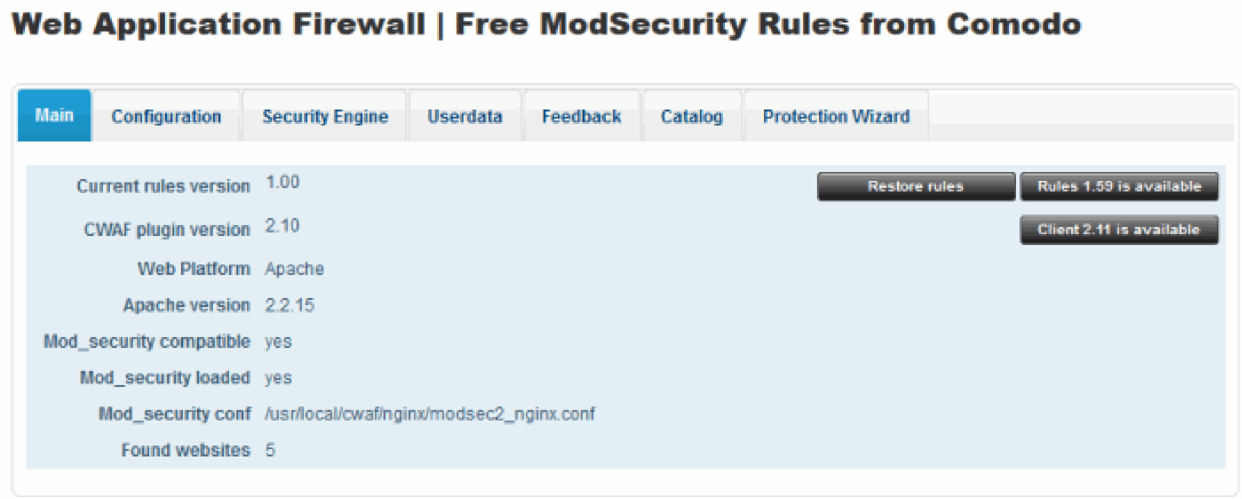
Access the CWAF cPanel plugin

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

The Comodo Web Application Firewall configuration screen will appear.

- Click the 'Main' tab

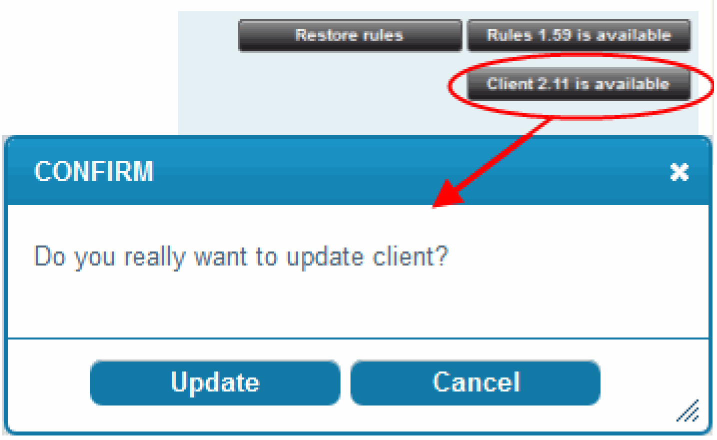
The 'Main' tab enables you to manually update the currently loaded rule set to the latest version or to restore to the previous version.



Web Application Firewall | Free ModSecurity Rules from Comodo

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

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



Do you really want to update client?

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

/var/log/CWAF/utils.log

- See the online help page **Use The Web Host Control Panel Plugin For Firewall Configuration** of the **Deploy CWAF Rules On Server** for more details on configuring the web application firewall through the plugin interface.

Access the CWAF DirectAdmin plugin

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

The Comodo Web Application Firewall configuration screen will appear.

The functionality and appearance of DirectAdmin Plugin is the same as for cPanel plugin.

- See the help page **Use The Web Host Control Panel Plugin For Firewall Configuration** of the **Deploy CWAF Rules On Server** for help with configuring the web application firewall through the plugin interface.

Access the CWAF Plesk plugin

- Login to Plesk on your server

- Click 'Extensions' > "Comodo WAF Plugin".

The Comodo Web Application Firewall configuration screen will appear.

The functionality and appearance of Plesk Plugin is the same as for cPanel plugin.

- See the online help page **Use The Web Host Control Panel Plugin For Firewall Configuration** of the **Deploy CWAF Rules On Server** for help with configuring the web application firewall through the plugin interface.

Access the CWAF Webmin plugin

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

The Comodo Web Application Firewall configuration screen will appear.

The functionality and appearance of Webmin Plugin is the same as for cPanel plugin.

- See the online help page **Use The Web Hosting Control Panel Plugin For Firewall Configuration** of the **Deploy CWAF Rules On Server** for help with configuring the web application firewall through the plugin interface.

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**