

Web Application Firewall
POWERED BY **COMODO**

Comodo Web Application Firewall for Plesk

Software Version 2.11

Administrator Guide

Guide Version 2.11.011320

Table of Contents

1. Comodo Free ModSecurity Rules for Plesk - Introduction.....	3
1.1. System Requirements.....	3
1.2. Signing up for Free ModSecurity Rules.....	3
2. Deploying Comodo ModSecurity Rule Set in Plesk.....	8
About Comodo Security Solutions.....	15

1. Comodo Free ModSecurity Rules for Plesk - Introduction

This guide explains how server administrators can use Plesk to download, implement and manage Comodo ModSecurity rule sets.

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 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.

CWAF has been tested on Apache and LiteSpeed on Linux servers. Versions for other web-server types are coming shortly.

CWAF is also integrated as a ModSecurity vendor in cPanel, DirectAdmin and Plesk panels and users can enable/disable Comodo protection rules and manage them with panel's internal tools.

Guide Structure

This guide is intended to take the administrator through the setup, configuration and use of Comodo Web Application Firewall in Plesk panel

- **Comodo Web Application Firewall - Introduction** - A high level description of the product
- **System Requirements** - List of compatible server environments for CWAF
- **Deploying Comodo ModSecurity Rule Sets in Plesk** - Guidance on downloading and deploying the firewall rule sets on to the server

1.1. System Requirements

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

- Apache 2 or LiteSpeed web server on RHLE, CentOS, CloudLinux, Debian, OpenSuSe and Ubuntu platform
- ModSecurity 2.7.5 and higher

1.2. Signing up for Free ModSecurity Rules

In order to enable Comodo ModSecurity Rules in Plesk, you need to have a Comodo Web Application Firewall account registered. 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 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 Com"/>
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 CWAF license, select 'Yes' for 'Are you an existing Comodo customer?'. You will need to fill only your username and password.

Customer Information (an * indicates required fields)

When paying by credit card, the billing information should be exactly as it appears on your credit card statement. For credit card verification, please ensure that your first and last name are entered as they appear on your card.

User Details

Are you an existing Comodo customer? Yes No

Email*

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

PayPal

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 use the same username and password you created or used during enrollment to activate Comodo ModSecurity Rule set in Plesk.

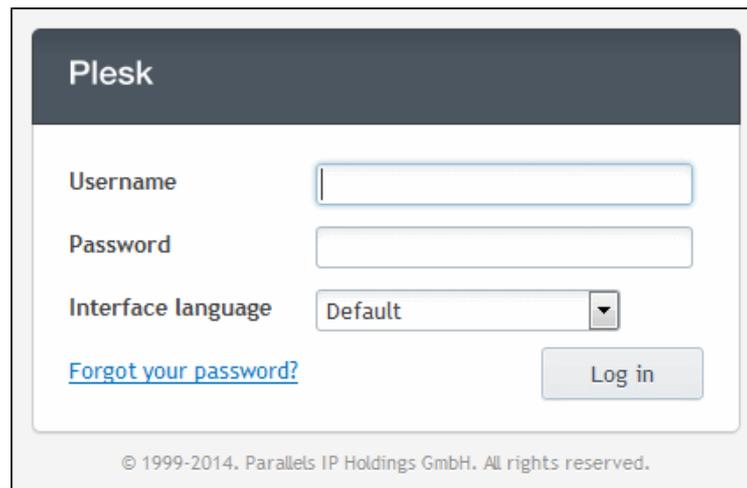
Further Reading:

- [Deploying Comodo ModSecurity Rule Set in Plesk](#)

2. Deploying Comodo ModSecurity Rule Set in Plesk

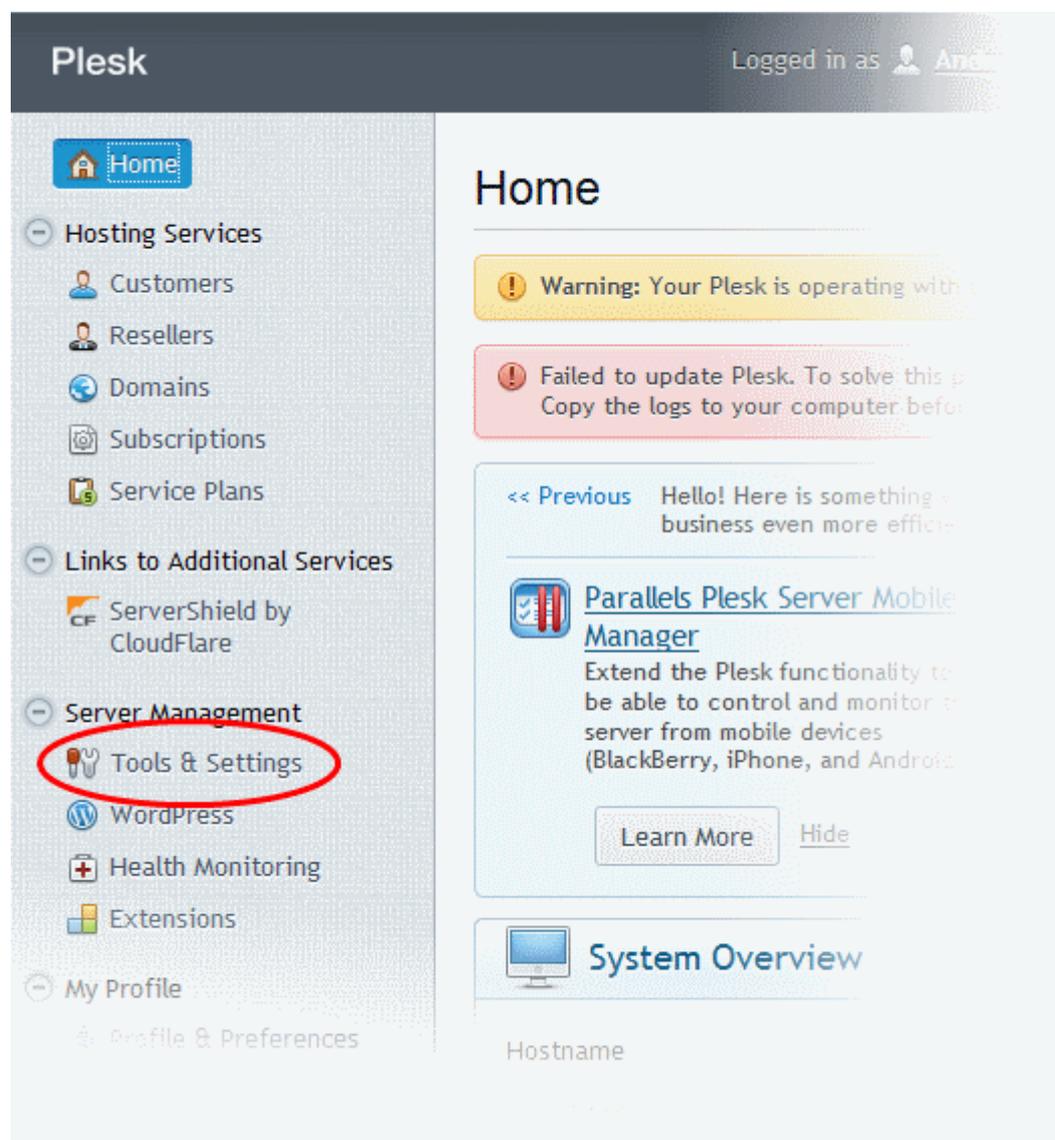
Comodo ModSecurity protection rules are now integrated in Plesk panel and can be activated from the 'Tools & Settings' feature.

- Sign in to your Plesk account



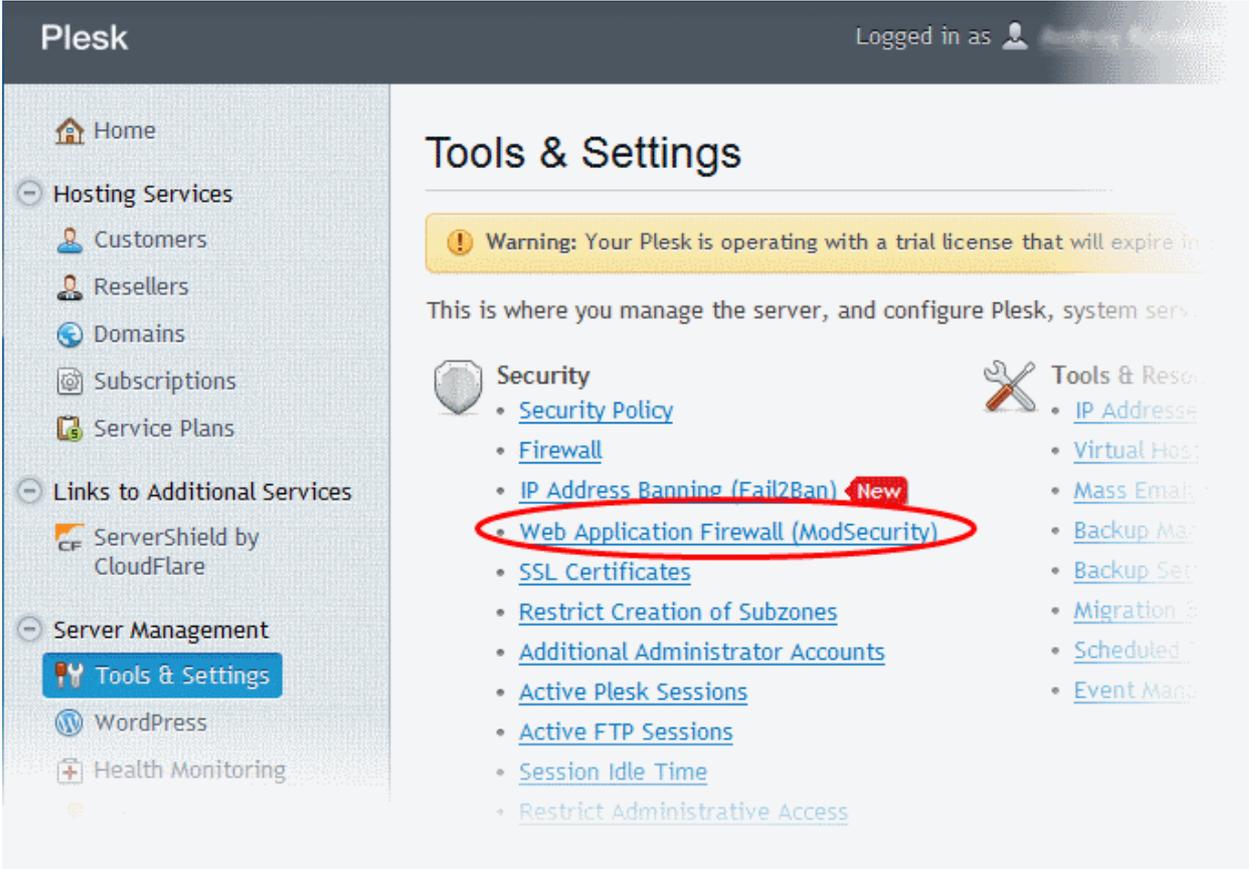
The image shows the Plesk login interface. It features a dark header with the word "Plesk" in white. Below the header, there are three input fields: "Username", "Password", and "Interface language" (a dropdown menu set to "Default"). A blue link for "Forgot your password?" is located below the password field. A "Log in" button is positioned to the right of the "Interface language" dropdown. At the bottom of the form, there is a copyright notice: "© 1999-2014. Parallels IP Holdings GmbH. All rights reserved."

- In the Plesk home page, click 'Tools & Settings' under 'Server Management'



The image is a screenshot of the Plesk home page. The top navigation bar includes the "Plesk" logo and the text "Logged in as Admin". A left sidebar contains a menu with categories: "Home", "Hosting Services" (Customers, Resellers, Domains, Subscriptions, Service Plans), "Links to Additional Services" (ServerShield by CloudFlare), "Server Management" (Tools & Settings, WordPress, Health Monitoring, Extensions), and "My Profile" (Profile & Preferences). The "Tools & Settings" item is circled in red. The main content area is titled "Home" and displays several widgets: a yellow warning box, a red error box, a "Hello!" message, a "Parallels Plesk Server Mobile Manager" advertisement, and a "System Overview" section.

- In the 'Security' section, click 'Web Application Firewall (ModSecurity)'



The screenshot shows the Plesk interface. The top navigation bar includes the Plesk logo and a user profile icon with the text 'Logged in as'. The left sidebar contains a menu with categories: Home, Hosting Services (Customers, Resellers, Domains, Subscriptions, Service Plans), Links to Additional Services (ServerShield by CloudFlare), and Server Management (Tools & Settings, WordPress, Health Monitoring). The main content area is titled 'Tools & Settings' and features a yellow warning banner: 'Warning: Your Plesk is operating with a trial license that will expire in...'. Below the banner, a text block states: 'This is where you manage the server, and configure Plesk, system services, and other tools.' The page is divided into two columns of links. The left column, under a shield icon and the heading 'Security', lists: Security Policy, Firewall, IP Address Banning (Fail2Ban) (with a 'New' badge), Web Application Firewall (ModSecurity) (circled in red), SSL Certificates, Restrict Creation of Subzones, Additional Administrator Accounts, Active Plesk Sessions, Active FTP Sessions, Session Idle Time, and Restrict Administrative Access. The right column, under a wrench icon and the heading 'Tools & Resources', lists: IP Address, Virtual Hosts, Mass Email, Backup Manager, Backup Settings, Migration & Cloning, Scheduled Tasks, and Event Manager.

- In the 'Web Application Firewall' interface, click the 'Change Rule Set' link beside 'Selected rule set' row.

Plesk

Logged in as [Admin](#) [Log out](#) [Help](#)

Home > [Tools & Settings](#) >

Web Application Firewall

Warning: Your Plesk is operating with a trial license that will expire in 8 days.

[General](#) [Settings](#)

Here you can configure the web application firewall (ModSecurity).

Web application firewall mode

- Off
Incoming HTTP requests and related responses are not checked.
- Detection only**
Each incoming HTTP request and the related response are checked against a set of rules. If the check succeeds, the HTTP request is passed to web site content. If the check fails, the event is logged, but no other actions are performed.
- On
Each incoming HTTP request and the related response are checked against a set of rules. If the check succeeds, the HTTP request is passed to web site content. If the check fails, the event is logged, a notification is sent, and the HTTP response is provided with an error code.

Selected rule set: Atomic Basic ModSecurity rule set [Change Rule Set](#)

[ModSecurity audit log](#)

The ModSecurity audit log file is the most useful piece of information in the system. When ModSecurity detects any event occurs, it generates an entry in the audit log file.

- The 'Settings' for Rules Set screen will be displayed. Select 'Comodo ModSecurity rule set (subscription)' from the options.

Plesk

Logged in as [Andreas Müller](#) [Log out](#) [Help](#)

Home > Tools & Settings >

Web Application Firewall

Warning: Your Plesk is operating with a trial license that will expire in 8 days.

[General](#) [Settings](#)

Rule sets

A rule set is a package that contains files with specific security rules. A security rule is checked by the web application firewall engine for each incoming HTTP request.

Rule set

- Atomic Basic ModSecurity rule set**
A tailored version of the Atomic ModSecurity rules, bundled with Plesk. Contains important security features and bug fixes released by GotRoot on a daily basis. These rules are fully supported and are recommended for production use.
- OWASP ModSecurity Core Rule Set (CRS)**
CRS provides generic protection from unknown vulnerabilities often found in web applications. This makes the difference between CRS and other intrusion detection and prevention systems, which rely on signatures specific to known vulnerabilities. However, OWASP rules might be too restrictive and thus block some functions, such as File Sharing, webmail, and some web applications.
- Atomic ModSecurity rule set (subscription)**
A monthly subscription to the latest version of the Atomic ModSecurity rules, with all the performance enhancements, new security features and bug fixes released by GotRoot on a daily basis. These rules are fully supported and are recommended for production use.
- Comodo ModSecurity rule set (subscription)**
Comodo Web Application Firewall (WAF) is a simple-to-use, customizable rules based traffic control system that protects your web based applications and prevents emerging hacking techniques with the use of frequently updated rules database. Comodo rule set requires a monthly subscription.
- Custom rule set**
Here you can upload a custom web application firewall rule set. You can use a trial package from Atomic ModSecurity.

- Next, you need to provide your credentials that was created during [sign up for CWAF](#).

security features and bug fixes released by GotRoot on a daily basis. These rules are fully supported and are recommended for production use.

Comodo ModSecurity rule set (subscription)

Comodo Web Application Firewall (CWAF) is a simple-to-use, customizable rules based traffic control system that protects your web based applications and prevents emerging hacking techniques with the use of frequently updated rules database. Comodo rule set requires a monthly subscription.

To enable this rule set:

1. [Register at Comodo site.](#)
2. Enter your username and password from this site.

Username *

Password *

Custom rule set

Here you can upload a custom web application firewall rule set. You can use a trial package from Atomic or a free package from Comodo. Supported formats: zip, tar.gz, tgz, tar.bz2, conf.

- If you have not signed up for CWAF, you can do so by clicking the 'Register at Comodo Site' link. Refer to the section '[Signing up for Free ModSecurity Rules](#)' for more details.
- Enter the CWAF username and password that was created during [signing up for CWAF](#) in the respective fields.
- Scroll down the page and click the 'OK' button at the bottom of the screen.

Tradeoff
The HTTP request URI, headers and the request POST data will be analyzed.

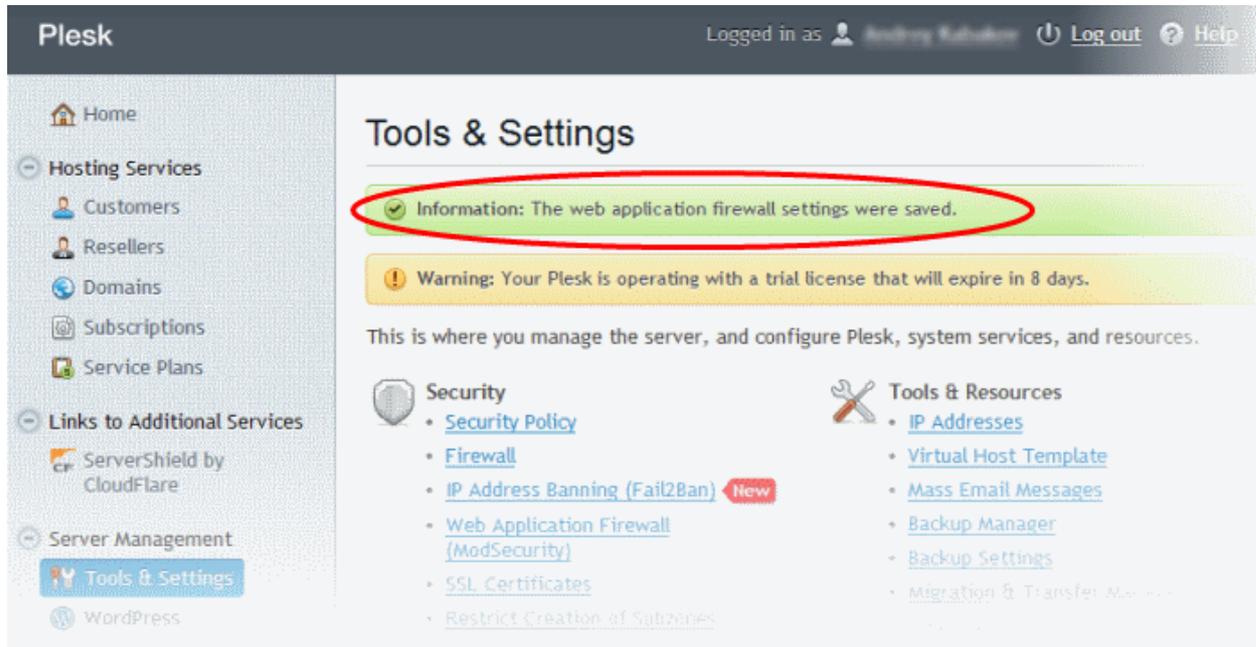
Thorough
The full HTTP request headers, the request POST data and the HTTP response body content will be analyzed.

Custom directives

Input a ModSecurity directive here. It will override the predefined directives (rule sets, specific rules, the predefined set of directives). For example: SecDebugLogLevel 6

* Required fields

The account details will be authenticated with Comodo and on successful verification, the Comodo ModSecurity Rule will be saved in the Plesk panel.



That's it. Comodo ModSecurity Rules Set is now activated in Plesk.

About Comodo Security Solutions

Comodo Security Solutions is a global innovator of cybersecurity solutions, protecting critical information across the digital landscape. Comodo provides complete, end-to-end security solutions across the boundary, internal network and endpoint with innovative technologies solving the most advanced malware threats. With over 80 million installations of its threat prevention products, Comodo provides an extensive suite of endpoint, website and network security products for MSPs, enterprises and consumers.

Continual innovation and a commitment to reversing the growth of zero-day malware, ransomware, data-breaches and internet-crime distinguish Comodo Security Solutions as a vital player in today's enterprise and home security markets.

About Comodo Cybersecurity

In a world where preventing all cyberattacks is impossible, Comodo Cybersecurity delivers an innovative cybersecurity platform that renders threats useless, across the LAN, web and cloud. The Comodo Cybersecurity platform enables customers to protect their systems and data against even military-grade threats, including zero-day attacks. Based in Clifton, New Jersey, Comodo Cybersecurity has a 20-year history of protecting the most sensitive data for both businesses and consumers globally. For more information, visit [comodo.com](https://www.comodo.com) or our [blog](#). You can also follow us on [Twitter](#) (@ComodoDesktop) or [LinkedIn](#).

1255 Broad Street

Clifton, NJ 07013

United States

Tel : +1.877.712.1309

Tel : +1.888.551.1531

<https://www.comodo.com>

Email: EnterpriseSolutions@Comodo.com