

Web Application Firewall

Feature Description

UPDATED: 27 July 2023

© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

These materials and all Progress® software products are copyrighted and all rights are reserved by Progress Software Corporation. The information in these materials is subject to change without notice, and Progress Software Corporation assumes no responsibility for any errors that may appear therein. The references in these materials to specific platforms supported are subject to change.

#1 Load Balancer in Price/Performance, 360 Central, 360 Vision, Chef, Chef (and design), Chef Habitat, Chef Infra, Code Can (and design), Compliance at Velocity, Corticon, Corticon.js, DataDirect (and design), DataDirect Cloud, DataDirect Connect, DataDirect Connect64, DataDirect XML Converters, DataDirect XQuery, DataRPM, Defrag This, Deliver More Than Expected, DevReach (and design), Driving Network Visibility, Flowmon, Inspec, Ipswitch, iMacros, K (stylized), Kemp, Kemp (and design), Kendo UI, Kinvey, LoadMaster, MessageWay, MOVEit, NativeChat, OpenEdge, Powered by Chef, Powered by Progress, Progress, Progress Software Developers Network, SequeLink, Sitefinity (and Design), Sitefinity, Sitefinity (and design), Sitefinity Insight, SpeedScript, Stylized Design (Arrow/3D Box logo), Stylized Design (C Chef logo), Stylized Design of Samurai, TeamPulse, Telerik, Telerik (and design), Test Studio, WebSpeed, WhatsConfigured, WhatsConnected, WhatsUp, and WS_FTP are registered trademarks of Progress Software Corporation or one of its affiliates or subsidiaries in the U.S. and/or other countries.

Analytics360, AppServer, BusinessEdge, Chef Automate, Chef Compliance, Chef Desktop, Chef Workstation, Corticon Rules, Data Access, DataDirect Autonomous REST Connector, DataDirect Spy, DevCraft, Fiddler, Fiddler Classic, Fiddler Everywhere, Fiddler Jam, FiddlerCap, FiddlerCore, FiddlerScript, Hybrid Data Pipeline, iMail, InstaRelinker, JustAssembly, JustDecompile, JustMock, KendoReact, OpenAccess, PASOE, Pro2, ProDataSet, Progress Results, Progress Software, ProVision, PSE Pro, Push Jobs, SafeSpaceVR, Sitefinity Cloud, Sitefinity CMS, Sitefinity Digital Experience Cloud, Sitefinity Feather, Sitefinity Thunder, SmartBrowser, SmartComponent, SmartDataBrowser, SmartDataObjects, SmartDataView, SmartDialog, SmartFolder, SmartFrame, SmartObjects, SmartPanel, SmartQuery, SmartViewer, SmartWindow, Supermarket, SupportLink, Unite UX, and WebClient are trademarks or service marks of Progress Software Corporation and/or its subsidiaries or affiliates in the U.S. and other countries. Java is a registered trademark of Oracle and/or its affiliates. Any other marks contained herein may be trademarks of their respective owners.

Please refer to the NOTICE.txt or Release Notes – Third-Party Acknowledgements file applicable to a particular Progress product/hosted service offering release for any related required third-party acknowledgements.

© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

Table of Contents

1 Introduction **5**

1.1 Document Purpose 6

1.2 Intended Audience 6

1.3 Legacy WAF Rules 6

2 Configuring WAF **7**

2.1 Resource Considerations 7

2.2 Balancing WAF Resource Utilization with High Load Applications 7

2.3 Managing Daily Updates 8

2.3.1 Automatic Downloading and Updating of Daily Updates 8

2.3.2 Manual Downloading and Updating of Daily Updates 10

2.4 Custom Rules 11

2.4.1 Delete/Download a Custom Rule or Data File 12

2.5 Configure WAF for a Virtual Service 13

2.5.1 Advanced Settings 15

2.5.2 False Positive Analysis 18

2.6 Backing Up and Restoring a WAF Configuration 20

2.7 WAF Logging, Statistics and Status Options 20

2.7.1 Export Logs in the Web Application Firewall menu 20

2.7.2 WAF Event Log 22

2.7.3 WAF Options in the Extended Log Files Screen 22

2.7.4 Enable WAF Debug Logging 24

© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

2.7.5 WAF Statistics 25
2.7.5.1 Home Page 25
2.7.5.2 Statistics Page 25
2.7.6 WAF Misconfigured Virtual Service Status 26
3 Troubleshooting 28
3.1 WAF Logging 28
3.2 WAF Compatibility with Kerberos Constrained Delegation (KCD) 28
3.3 Unable to Download/Update Daily Updates 28
Appendix A: Legacy Rules 30
Configure WAF Options (Legacy) for a Virtual Service 30
WAF Options (Legacy) in the Virtual Service Modify Screen 32
References 37
Last Updated Date 38

© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

1 Introduction

With cybercriminal attacks on the rise, organizations need to do more than ever to mitigate risks to their applications on the web. Application security is a multifaceted and ever-changing task and must be applied at multiple levels of the infrastructure that serves applications. Security must be provided on the network before requests reach the backend application servers, and Kemp has the experience and the tools you need to do this. Deploying LoadMaster with the Kemp Web Application Firewall (WAF) enabled as part of your network infrastructure helps deliver in-depth security for your web servers and applications.

The Kemp Web Application Firewall (WAF) enables secure deployment of web applications, preventing Layer 7 attacks while maintaining core load balancing services, ensuring comprehensive application delivery and security. WAF functionality directly augments the LoadMaster's existing security features to create a layered defense for web applications - enabling a safe, compliant and productive use of published services.

> WAF is only available on certain subscriptions. Please contact a Kemp representative if needed.

When WAF is enabled, the WAF engine scans every incoming HTTP packet – running through each assigned rule individually and deciding what action to take if a rule is triggered. The rules can be run on requests and responses.

WAF can protect against attacks, such as:

- SQL Injection
- Cross-Site Scripting (XSS)
- Unvalidated redirects and forwards
- Missing function-level access control
- Sensitive data exposure

For a more detailed overview of the WAF feature, refer to the WAF section in the **Kemp LoadMaster, Product Overview** on the Kemp Documentation page.

© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

1.1 Document Purpose

The purpose of this document is to describe the WAF features and provide step-by-step instructions on how to configure the WAF settings in the Kemp LoadMaster.

For further information and assistance, refer to our Kemp Support site for Support contact details: http://kemptechnologies.com/load-balancing-support/kemp-support/.

1.2 Intended Audience

This document is intended to be read by anyone interested in finding out more about the Kemp WAF functionality.

1.3 Legacy WAF Rules

From LMOS version 7.2.54, there is new functionality allowing the use of OWASP rules. This document mainly provides details on the newer functionality, but for details on how to configure the legacy WAF rules, the only rules available on LoadMaster versions prior to 7.2.54, please refer to **Appendix A - Legacy Rules**.

Legacy WAF rules were retired on 29th June 2021 and no further updates are available. Kemp encourages users to migrate their configuration to the new WAF service.

© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

2 Configuring WAF

2.1 Resource Considerations

> Utilizing WAF can have a significant performance impact on the LoadMaster deployment. Please ensure that the appropriate resources are allocated.

For virtual and bare metal LoadMaster instances, a minimum of 2GB of allocated RAM is required for the operation of WAF. The default memory allocation for Virtual LoadMasters and LoadMaster Bare Metal instances before LoadMaster Operating System version 7.1-22 is 1 GB of RAM. If this default allocation has not been changed, modify the memory settings before proceeding with the WAF configuration. If the check box to enable WAF is grayed out, it could mean that the LoadMaster does not have enough memory to run WAF.

There is a WAF engine open connection limit of 64000 per Virtual Service.

> To reduce the risk of the WAF connection limit being reached, connections will be closed after 20 seconds when a remote log server is too slow to respond. There is no impact on connections in use.

2.2 Balancing WAF Resource Utilization with High Load Applications

The WAF subsystem uses a significant amount of system resources. When enabling WAF, you should avoid overconsuming system resources that are needed for load balancing Virtual Services. When WAF starts to consume resources at a level that impacts overall system performance, one or more of these symptoms can be observed:

- High CPU utilization
- High memory utilization
- InterProcess Communication (IPC) issues between Layer 7 and WAF processes
- Decreased Virtual Service throughput
- Increased Virtual Service latency

There are essentially two ways of dealing with these issues:

© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

- Disable WAF completely on one or more Virtual Services.
- Tailor the applied rulesets used on each Virtual Service to reduce the rules applied to the minimum necessary for secure operation.

The best practice for WAF rulesets is to avoid a blanket application of a ruleset and instead, enable only those rules in the ruleset that are specifically required for your application.

Note that internal processing and communication between WAF and Layer 7 in version 7.2.36 is enhanced to help mitigate resource exhausting issues through smarter thread and resource management. The best practice is still to enable a minimum set of rules instead of enabling the entire ruleset.

2.3 Managing Daily Updates

The Kemp-provided daily updates can be set to download automatically and install. They can also be manually downloaded and installed. The sections below explain how to use each method.

> The IP/FQDN and port of the Kemp licensing server must be open on your firewall. The FQDN and IP address is **licensing.kemp.ax 52.166.52.190**, and the port is **443**. The old FQDNs for the Kemp licensing server are **alsi.kemptechnologies.com** and **alsi2.kemptechnologies.com**, and the IP address for the old FQDNs is **52.136.251.129**. These also may need to be open depending on your LoadMaster version.

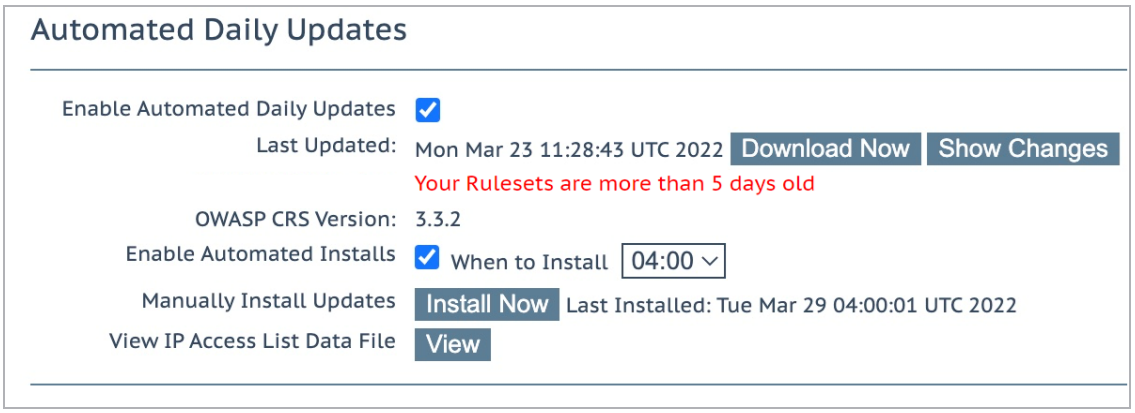
> Kemp-provided daily updates are only available when you have an Enterprise Plus subscription. For further details on the subscription tiers, go to LoadMaster Support Subscriptions.

2.3.1 Automatic Downloading and Updating of Daily Updates

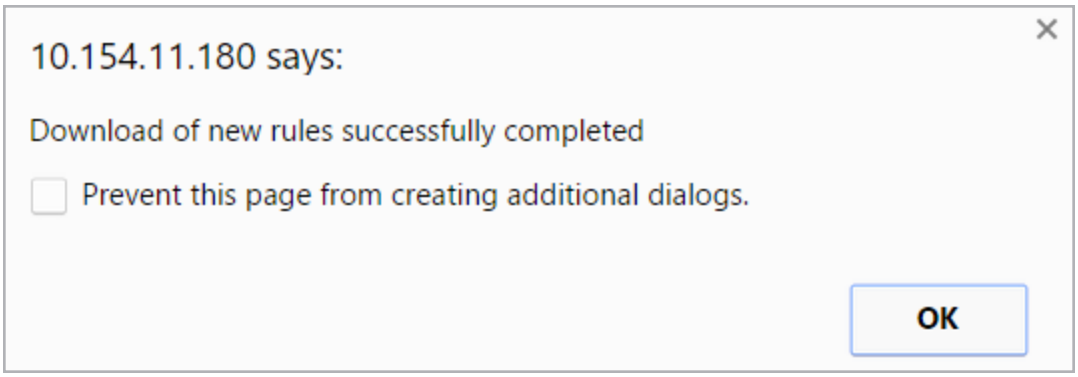
Before enabling the automatic installation of daily updates, you must first download and install the latest updates. Follow the steps below to configure automatic download and installation settings for latest updates:

1. In the main menu, select **Web Application Firewall > Access Settings**.

© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

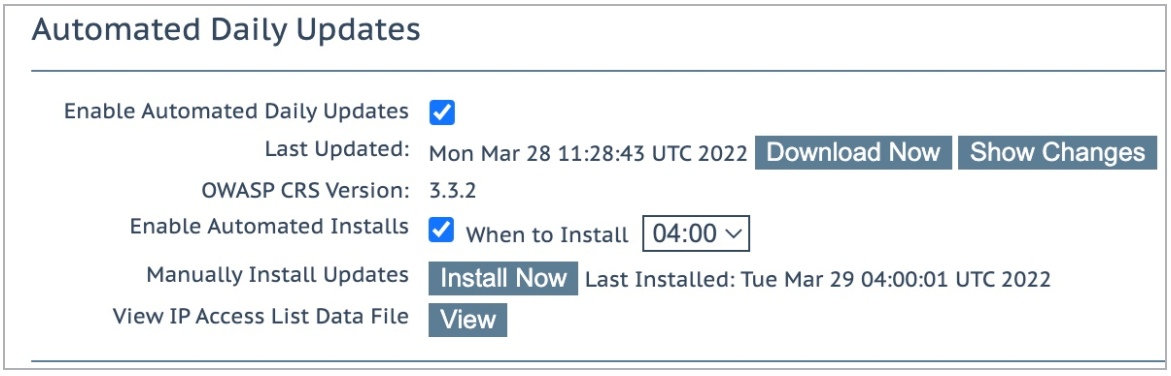


2. Click the **Download Now** button to download the latest daily updates.



3. Click **OK** on the success message.

4. Click **Install Now** to install the latest daily updates.



5. To enable the automatic download of daily updates, select the **Enable Automated Daily Updates** check box.

© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

> The **Download Now** and **Install Now** options are grayed out if WAF support license has expired. If this is the case, contact Kemp to renew your subscription.

6. To enable automatic installation of the daily updates, select the **Enable Automated Installs** check box.

   By default, the **Enable Automated Installs** and **Manually Install Updates** options are grayed out. The rules must be downloaded for the first time before these options become available.

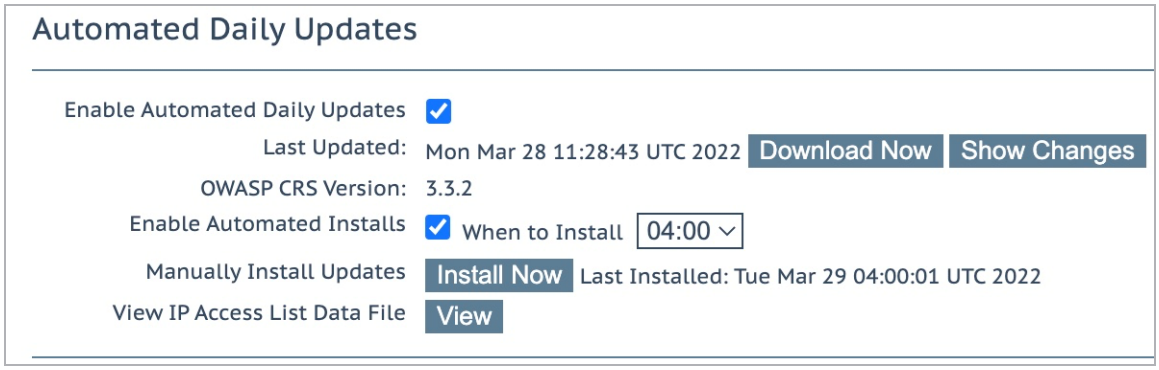
7. Select the time (hour of the day) to install the daily updates automatically.

   The daily updates must be assigned to a Virtual Service to take effect.

2.3.2 Manual Downloading and Updating of Daily Updates

To manually download and install the daily updates, follow the steps below:

1. In the main menu, select **Web Application Firewall > Access Settings**.



2. Click **Download Now** to download the daily updates now.

   A warning message appears if the rules have not been updated in the last seven days or if they have not been downloaded at all.

3. After the daily updates are downloaded, the **Show Changes** button appears. Click this button to retrieve a log of changes that have been made to the Kemp WAF rule set.

4. Click **Install Now** to install the daily updates manually.

> The daily updates must be assigned to a Virtual Service in order to take effect.

© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

2.4 Custom Rules

Third-party rules can be uploaded to the LoadMaster. You can also write your own custom rules, which can be uploaded. These rules must be in the ModSecurity rule format in order to upload correctly. The **Custom Rules** screen enables you to upload **WAF Custom Rules** (.conf) and associated **WAF Custom Rule Data** (.data or .txt) files. The file name can contain alphanumeric characters and the following special characters: -. _ You can also upload gzip-compressed Tarball files (.tar.gz), which contain multiple rule and data files.

> Kemp does not recommend using the WAF rule "redirect" action in custom rules because of the impact this has on system performance. You should use content rules instead for that purpose.

> Based on OWASP recommended best practices, the order of WAF rule processing was changed in LoadMaster firmware version 7.2.57. As of 7.2.57, custom rules are processed before the OWASP CRS rules.

To check the order that the rules are processed in:

1. Navigate to **System Configuration > Logging Options > System Log Files > Debug Options** and click the **Enable Logging** button next to **Enable WAF Debug Logging**.

2. When WAF debug logging is enabled, if there are WAF debug logs - the option **WAF Debug Log File** becomes available in the **System Log Files** screen. Click **View** to view the WAF debug log file.

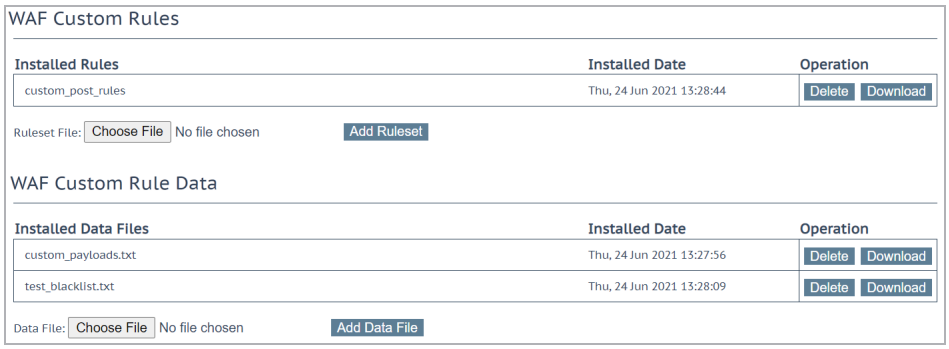
3. You can see what order the rules are processed in. Lines that say **Invoking rule** specify when the rule was processed.

> Please be aware that enabling WAF debug logging option will generate logs that may include Personally Identifiable Information as defined under the General Data Protection Agreement (EU GDPR). You should follow your organization's best practice to protect this information which may include anonymizing, deleting, or encrypting the data within the logs.

To upload rule and data files, follow the steps below:

4. In the main menu, select **Web Application Firewall > Custom Rules**.

© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.



5. To upload custom rules; in the **Installed Rules** section, click **Choose File**.

   Individual rules can be uploaded as .conf files. Alternatively, you can load a package of rules in a .tar.gz file.

6. Browse to and select the rule file(s) to be uploaded.

7. Click **Add Ruleset**.

8. To upload any additional data files, in the **WAF Custom Rule Data** section, click **Choose File**.

   The additional files are for the rules' associated data files. If you uploaded a Tarball in the **Browse to and select the rule file(s) to be uploaded.** step, the rules and data files can be packaged together.

9. Browse to and select the additional data files to be uploaded.

10. Click **Add Data File**.

The rules are now available to assign within the Virtual Services modify screen. Refer to the next section to determine how to configure the Virtual Service to use the installed rules.

2.4.1 Delete/Download a Custom Rule or Data File



Custom rules and data files can be deleted or downloaded by clicking the relevant buttons.

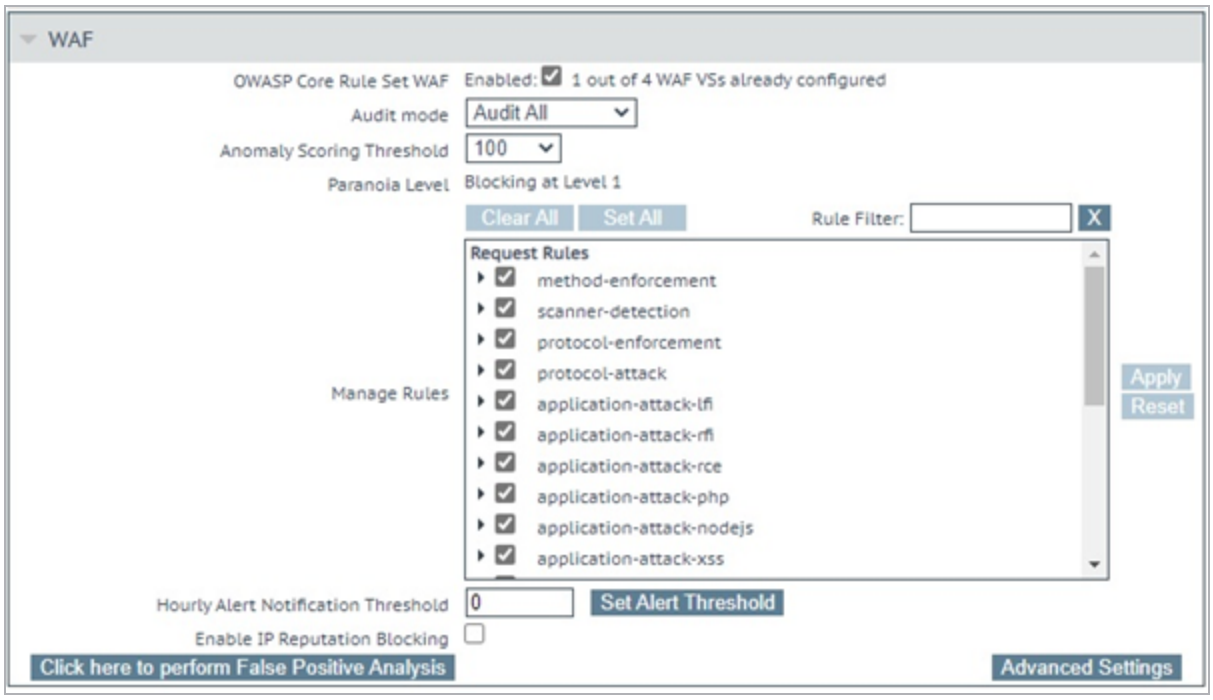
> If a rule is assigned to a Virtual Service, it will not be available for deletion.

© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

2.5 Configure WAF for a Virtual Service

WAF settings can be configured for each Virtual Service. Follow the steps below to configure the WAF in a Virtual Service.

1. In the main menu of the LoadMaster UI, select **Virtual Services >View/Modify Services**.
2. Click **Modify** on the relevant Virtual Service.
3. Expand the **WAF** section.



4. By default, WAF is disabled. To enable WAF, select **Enabled**.

When WAF is enabled for a Virtual Service, the section heading in the Virtual Service options changes from **WAF** to **WAF - Enabled**

The maximum number of WAF-enabled Virtual Services is the total (unused or available) RAM (in MB)/512 MB. For example: 8 GB/512 MB = 16 WAF-enabled Virtual Services. When the maximum is reached, no additional Virtual Services can be enabled with WAF.



A message displays if there is insufficient memory available to enable WAF.

© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

A message is displayed next to the **Enabled** check box displaying how many WAF-enabled Virtual Services exist and the maximum number of WAF-enabled Virtual Services that can exist. If the maximum number of WAF-enabled Virtual Services is reached, the **Enabled** check box is grayed out.

5. Specify the **Audit mode**.

There are three audit modes:
- **No Audit:** No data is logged.
- **Audit Relevant:** Logs data that is of a warning level and higher. This is the default option for this setting.
- **Audit All:** Logs all data through the Virtual Service.

Selecting the **Audit All** option produces a large amount of log data. Kemp does not recommend selecting the **Audit All** option for normal operation. However, the **Audit All** option can be useful when troubleshooting a specific problem.

6. Specify the **Anomaly Scoring Threshold**.

> For each request, every triggered detection raises the anomaly score, most rules having a score of 5. If the cumulative anomaly score per request hits the configured limit, the request will be blocked. The default value is 100 and allowable range is 1 to 10000.

7. The Paranoia Level can be set in **Advanced Settings**, but the value is displayed here for informational purposes.

8. Enable or disable rules in the **Manage Rules** section. When finished making changes, click **Apply**.

Rules are grouped in the **Request Rules** section as per the OWASP numbering system. Rule groups or Individual rules within each ruleset can be enabled/disabled as required. To enable a rule or group of rules, select the relevant check box. If you have previously enabled/disabled rules in that ruleset, within that Virtual Service – the rules retain their previous settings.

> Some rules or rule sets may have dependencies on other rules. There is no dependency check in the LoadMaster when rules are disabled - before disabling any rule, be aware of any rule chains or dependencies.

© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

There is a **Run First** check box available for custom rules. If the **Run First** check box is enabled for a custom rule, the rule will be run first, before the OWASP Core Rule Set (CRS). If the **Run First** check box is disabled for a custom rule, the custom rule runs after the CRS.

In the **Workloads** section there are several workloads available.

If a user has created custom rules, they can be enabled or disabled within the **Custom Rules** section.

To filter rules enter text into the **Rule Filter** text box and only rules containing that text will be shown. You can select the filtered rules by clicking **Set All** or deselect the filtered rules by clicking **Clear All**. Click the **Apply** button to apply the changes.

Clicking **Reset** will reverse any changes that you have made that have not been applied.

9. Specify the **Hourly Alert Notification Threshold** and click **Set Alert Threshold**.

   This is the number of incidents per hour before sending an alert. Setting this to **0** disables alerting.

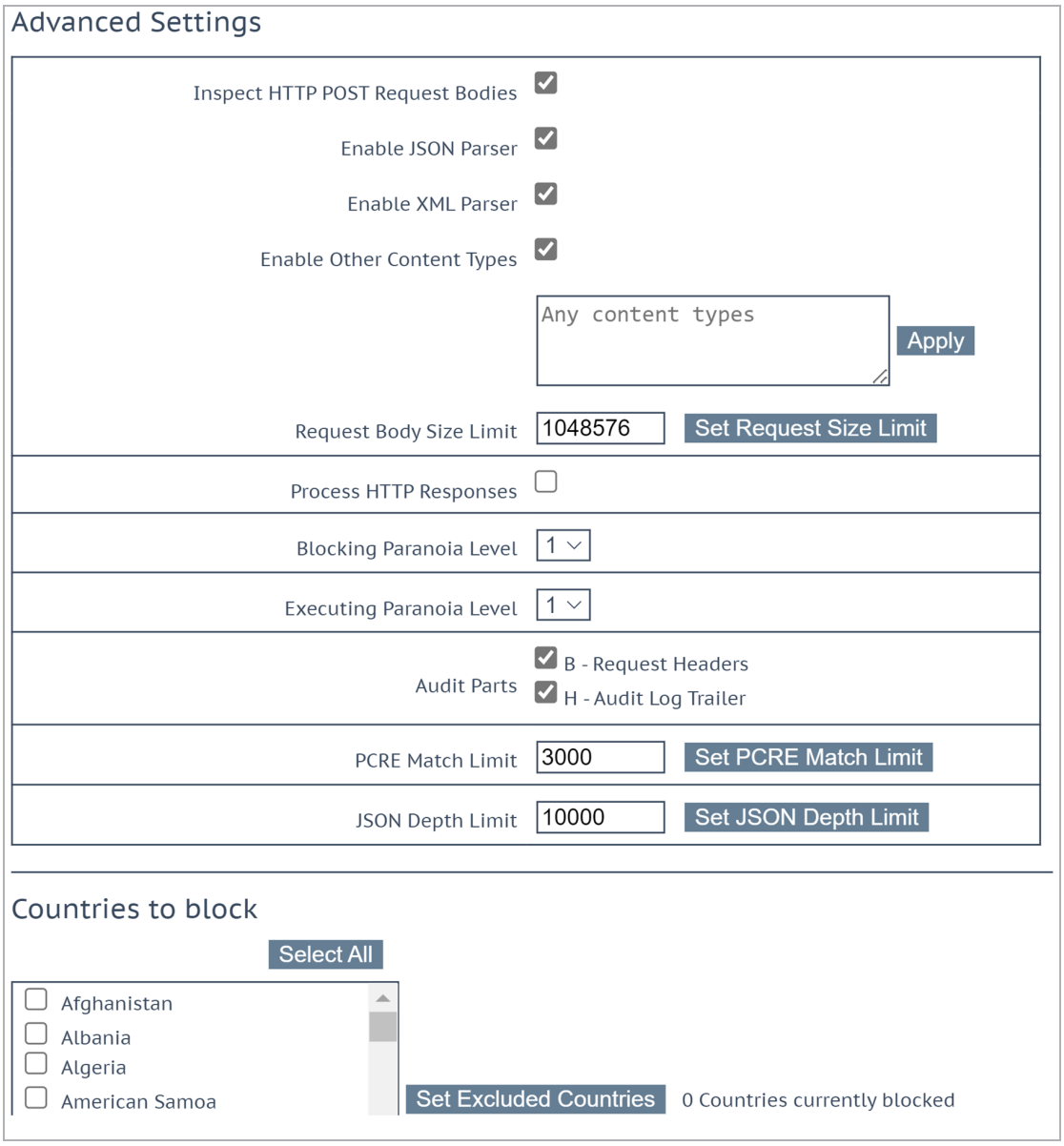
10. To enable the **IP Reputation Blocking** rule set, select the **IP Reputation Blocking** check box.

    This **IP Reputation Blocking** rule set enables the checking of client addresses against the IP reputation database.

2.5.1 Advanced Settings

Click the **Advanced Settings** button to configure the advanced OWASP settings.

© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.



1. Specify whether or not to **Inspect HTTP POST Request**.

   The **Inspect HTTP POST Request option** is disabled by default. If you enable this option, three more check boxes become available that allow you to enable the processing of JavaScript Object Notation (JSON), Extensible Markup Language (XML) requests, and other content types.

2. **Request Body Size Limit**: This option allows you to set the maximum size of POST request bodies that the WAF engine will allow through. Higher values require more memory

© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

resources and may impact WAF engine performance. The default value is 1048576 bytes. The range of valid values is 1024 to 52428800.

3. Select **Process HTTP Responses** to enable checking of the responses from the server to the client.

Enabling the **Process HTTP Responses** option makes two more options, **E - Intended Response Body** and **F- Response Headers**, available in the **Audit Parts** options

The processing of response data can be CPU and memory intensive and may impact on performance.

4. Select the **Blocking Paranoia Level** to define how strictly the ModSecurity engine implements each rule.

The default Paranoia Level value is set at 1. With each paranoia level increase, the CRS enables stricter implementations of the rules, giving you a higher level of security. However, higher paranoia levels also increase the possibility of blocking some legitimate traffic due to false positives. If you use higher paranoia levels, you will likely need to add some exclusion rules for certain applications that need to receive complex input patterns.

5. Select the **Executing Paranoia Level** that defines the paranoia level at which the ModSecurity engine checks/verifies the requests coming from the servers. The results of the checks will be logged but the **Executing Paranoia Level** is not used to determine what traffic will be blocked.

Though the **Executing Paranoia Level** can be higher than the **Blocking Paranoia Level**, it cannot be lower. A higher **Executing Paranoia Level** enables users to see which rules would be triggered at a higher Paranoia level without blocking traffic.

6. **Audit Parts**: A single string that contains the sections that are to be entered in the WAF audit log for each request. The supported values are A, B, E, F, H, K, Z,though only the values B, E, F, H can be enabled or disabled.

For further information regarding the Audit Parts, please refer to https://github.com/SpiderLabs/ModSecurity/wiki/ModSecurity-2-Data-Formats

7. **PCRE Match Limit**: Set the PCRE Match Limit value and click the Set PCRE Match Limit button. The default value is 10000. The maximum value is 9999999.

This setting sets the maximum iterations that the internal PCRE engine uses before failing a match. A lower value may cause a valid match to fail, whereas a higher value may cause the WAF engine to run slower. This setting can be used to protect against Denial of Service (DoS) attacks using complex regular expressions.

© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

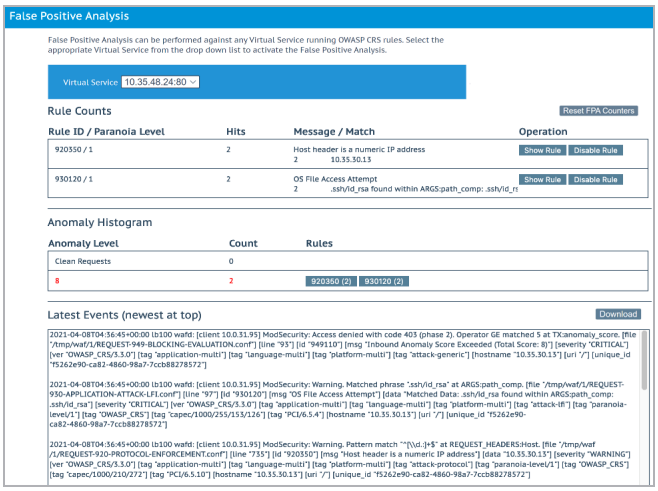
8. **JSON Depth Limit**: Set the JSON Depth Limit value and click **Set JSON Depth Limit**. The default value is 10000.

   This value sets the maximum depth that will be accepted during JSON parsing. Lower values may cause a valid match to fail. Higher values may cause the WAF engine to run slower. The range of valid values is 1000 to 99999.

9. **Countries to block**: Based on GEO IP information, you can select countries that should not be allowed access. Click the **Select All** button to block the access for all countries or select individual countries from the country list that are to be blocked and click the **Set Excluded Countries** button.

2.5.2 False Positive Analysis

This feature allows users to perform false positive analysis against their applications to obtain enhanced visibility of attacks and fine-tune protection. Click the **Click here to perform False Positive Analysis** button to check False Positives against any virtual service that runs OWASP CRS rules.



Rule Counts

The Rule Counts section displays information on any rules that are being triggered by requests. Displays the Rule ID, the paranoia level the rule is running under, the number of hits per requests that have triggered the rule and the message or match for the request are displayed for each rule that is triggered.

© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

Clicking the **Show Rule** button in the **Operation** column displays the contents of the rule file associated with the triggered rule. This opens in a separate tab and the URL contains the triggered rule id.

The rule can be disabled by clicking the **Disable Rule** button.

Reset FPA Counter

Reset all False Positive Analysis Counters (Anomaly Histogram and Latest Events) for the virtual service. Clearing the Latest Events does not remove the logs from the LoadMaster, they are still available under **System Configuration > Logging Options > System Log Files > WAF Event Log File**.

Anomaly Histogram

The first row of the **Anomaly Histogram** section displays how many requests have been run without triggering a rule.

Each subsequent row gives details of rules that have been triggered and which are affecting the Anomaly Score. In each row the cumulative Anomaly Score, the number of requests which have triggered the rule and the rule details are provided

Latest Events (newest at top)

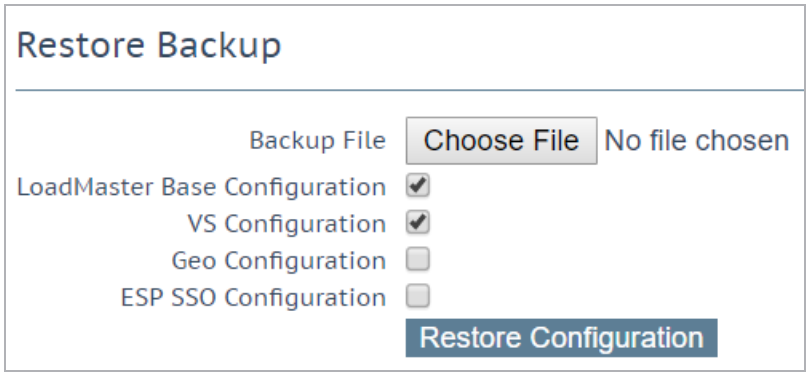
Displays the event details for each rule that is triggered. These messages are in the standard ModSecurity log format and contains the anomaly score, the warning message, the attack state, and the paranoia level.

Download

Click the **Download** button to download the displayed WAF event logs details.

© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

2.6 Backing Up and Restoring a WAF Configuration



A backup of the LoadMaster configuration can be taken by going to **System Configuration > System Administration > Backup/Restore** and clicking **Create Backup File**.

The configuration can be restored from this screen also. Note that the Virtual Service settings can be restored by selecting **VS Configuration**, and the rules can be restored by selecting **LoadMaster Base Configuration**.

> The base configuration preserves the IP configuration information. The IP configuration information will need to be reconfigured when you restore the LoadMaster Base Configuration

> A WAF configuration can only be restored onto a LoadMaster with a WAF license.

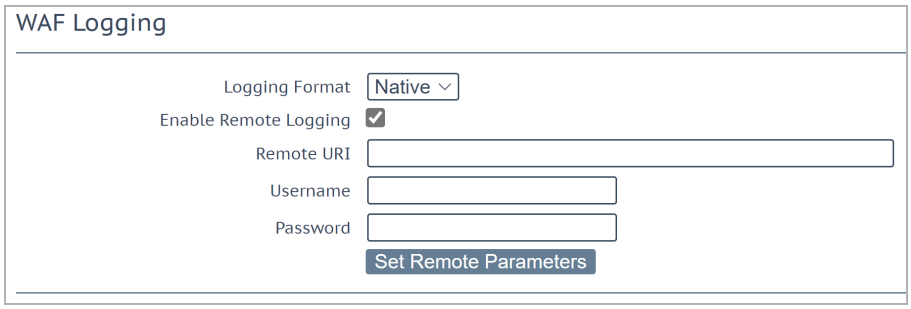
2.7 WAF Logging, Statistics and Status Options

This section describes the WAF Logging, Statistics and Status options available in the LoadMaster UI.

2.7.1 Export Logs in the Web Application Firewall menu

You can get to this screen by selecting **Web Application Firewall > Export Logs** in the main menu of the LoadMaster UI.

© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.



Logging Format

Select either Native or JSON depending on what format you want the audit logs to appear.

Enable Remote Logging

This check box enables you to enable or disable remote logging for WAF.

Remote URI

Specify the Uniform Resource Identifier (URI) for the remote logging server.

Username

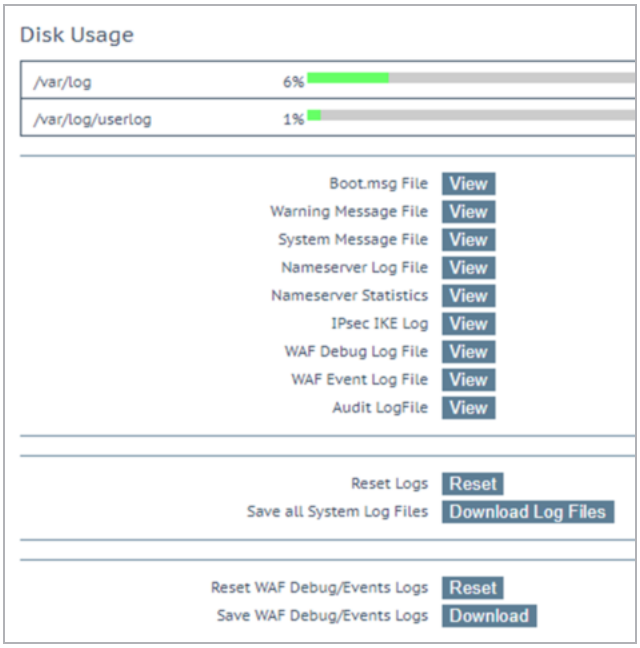
Specify the username for the remote logging server.

Password

Specify the password for the remote logging server.

© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

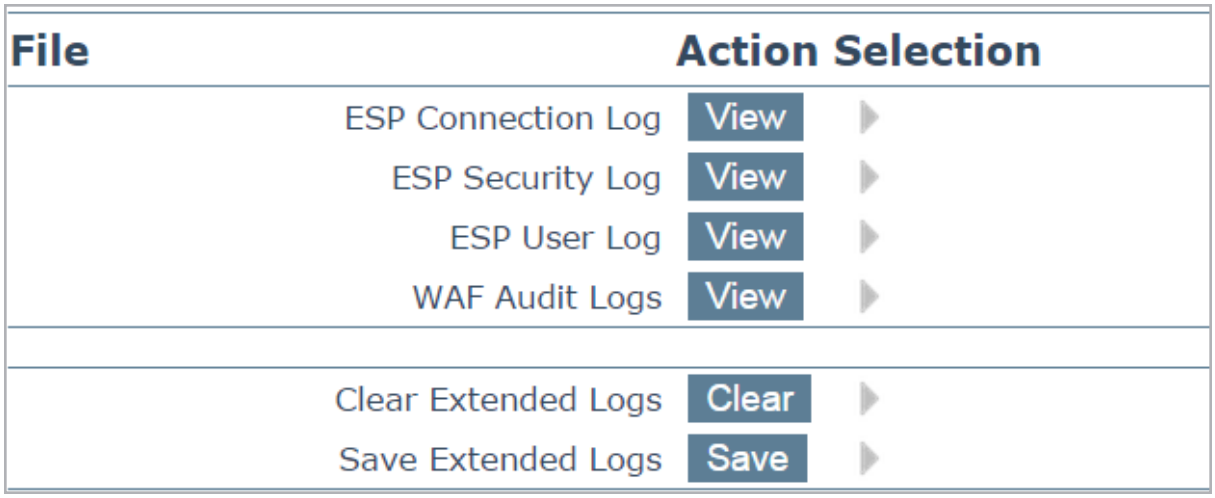
2.7.2 WAF Event Log



You can view the WAF Event Log by going to **System Configuration > Logging Options > System Log Files** and clicking the relevant **View** button. This log file contains all WAF alerts and automatically updates to show new events.

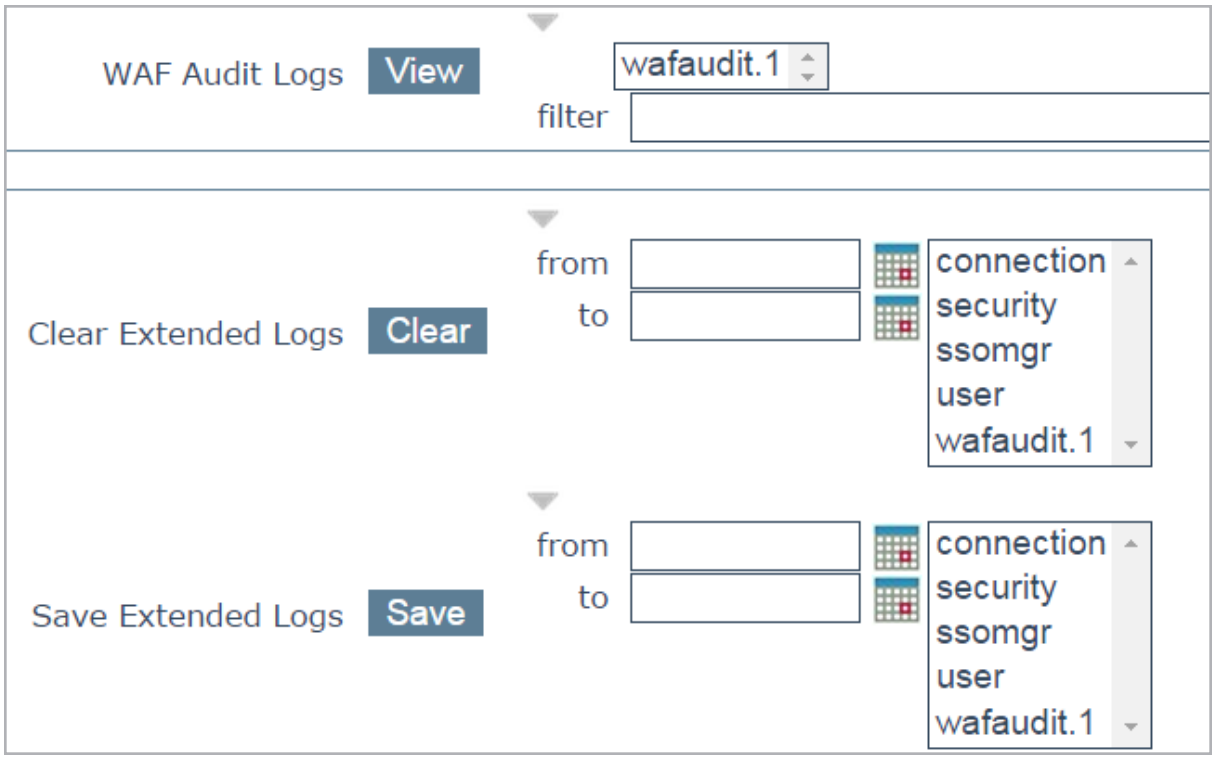
You can also reset and/or download the WAF debug/event logs by clicking the relevant buttons.

2.7.3 WAF Options in the Extended Log Files Screen



© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

The **Extended Log Files** screen provides options for logs relating to the ESP and WAF features. These logs are persistent and will be available after a LoadMaster reboot. To view all of the options click the icons.



> In addition to WAF logs, ESP logs are also available on this screen. For more information, refer to the **Edge Security Pack (ESP), Feature Description** on the Kemp Documentation page.

WAF Audit Logs: recording WAF logs based on what has been selected for the **Audit mode** drop-down list (either **Audit Relevant** or **Audit All**) in the **WAF Options** section of the Virtual Service modify screen.

To view the logs, select the appropriate log file and click the relevant **View** button.

The number listed in each log entry corresponds to the ID of the Virtual Service. To get the Virtual Service ID, first ensure that the API interface is enabled (**Certificates & Security > Remote Access > Enable API Interface**). Then, in a web browser address bar, enter **https://<LoadMasterIPAddress>/access/listvs**. Check the **index** of the Virtual Service. This is the number that corresponds to the number on the audit log entry.

© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

One or more archived log files can be viewed by selecting the relevant file(s) from the list of file names and clicking the **View** button. You can filter the log files by entering a word(s) or regular expression in the **filter** field and clicking the **View** field.

Clear Extended Logs

All extended logs can be deleted by clicking the **Clear** button.

Specific log files can be deleted by filtering on a specific date range, selecting one or more individual log files in the log file list or selecting a specific log type (for example, connection, security or user) in the log file list and clicking the **Clear** button. Click **OK** on any warning messages.

Save Extended Logs

All extended logs can be saved to a file by clicking the **Save** button.

Specific log files can be saved by filtering on a specific date range, selecting one or more individual log files in the log file list or selecting a specific log type (for example connection, security or user) in the log file list and clicking the **Save** button.

2.7.4 Enable WAF Debug Logging

You can enable logging to get detailed information about traffic that is analyzed by Web Application Firewall. Information that is contained in the logs includes the time that LoadMaster WAF received the request from your LoadMaster resource, detailed information about the request, and the action for the rule that each request matched.

To enable the WAF debug traces, click the **Enable Logging** button at **System Configuration > Logging Options > System Log Files > Debug Options**.

> Please be aware that enabling this option will generate logs that may include Personally Identifiable Information as defined under the General Data Protection Agreement (EU GDPR). You should follow your organization's best practice to protect this information which may include anonymizing, deleting, or encrypting the data within the logs.

> This generates a lot of log traffic. It also slows down WAF processing. Only enable this option when requested to do so by Kemp Technical Support. Kemp does not recommend enabling this option in a production environment.

© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

The WAF debug logs are never closed, and they are rotated if they get too large. WAF (in general) needs to be disabled and re-enabled (by clearing and re-selecting the **Enabled** check box) in all WAF-enabled Virtual Service settings to re-enable the debug logs. Alternatively, perform an update (in the **Web Application Firewall > Custom Rules** screen), with daily updates that are relevant for the Virtual Service(s).

2.7.5 WAF Statistics

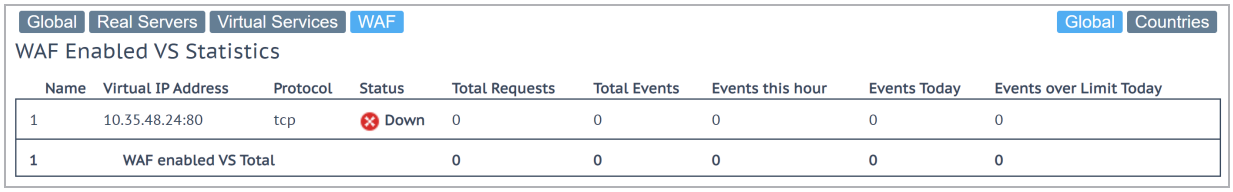
2.7.5.1 Home Page



The **WAF Status** section is displayed on the UI home page if at least one Virtual Service has WAF enabled. The values shown here are as follows:

- The total number of requests handled by the WAF shows all requests, whether they were blocked or not. Two requests are recorded for each connection – one incoming and one outgoing request.
- The total number of events handled by the WAF, therefore requests that were blocked.
- The number of events that have happened in the current hour since xx.00.00.
- The number of events that have happened since 00.00 am local time.
- The number of times the event counter has gone over the configured warning threshold today. For example, if the threshold is set to 10 and there have been 20 events, this counter will be set to 2. The warning threshold is set on a per-Virtual Service basis by filling out the **Hourly Alert Notification Threshold** field in either **WAF Options (Legacy) or WAF sections** in the Virtual Service modify screen.

2.7.5.2 Statistics Page



© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

To get to the WAF statistics page in the LoadMaster UI, go to **Statistics > Real Time Statistics > WAF > Global**. These statistics refresh every 5 to 6 seconds. The following items are displayed on this screen:

Count: The left-most column displays the total number of WAF-enabled Virtual Services.

Name: The name of the WAF-enabled Virtual Service.

Virtual IP Address: The IP address and port of the Virtual Service.

Protocol: The protocol of the Virtual Service (tcp or udp).

Status: Displays the status of the Virtual Service. For information on each of the possible statuses, refer to the **Web User Interface (WUI), Configuration Guide** on the Kemp Documentation page.

Total Requests: The total number of requests handled by the WAF and shows all requests, whether they were blocked or not. Two requests are recorded for each connection – one incoming and one outgoing request.

Total Events: The total number of events handled by the WAF (therefore, requests that were blocked).

Events this hour: The number of events that have happened in the current hour since xx.00.00.

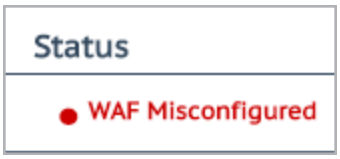
Events Today: The number of events that have happened since 00.00 am local time.

Events over Limit Today: The number of times the event counter has gone over the configured warning threshold today. For example, if the threshold is set to 10 and there have been 20 events, this counter will be set to 2. The warning threshold is set on a per-Virtual Service basis by filling out the **Hourly Alert Notification Threshold** field in either **WAF Options (Legacy) or WAF sections** in the Virtual Service modify screen.

Countries: Click the **Countries** button in the top right of the page to display the screen that contains a list of top 10 blocked countries.

These WAF statistics can also be seen in the Virtual Service statistics screen (go to **Statistics > Real Time Statistics > Virtual Services** and then click the **Virtual IP Address** link).

2.7.6 WAF Misconfigured Virtual Service Status



© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

On the **View/Modify Services** screen in the LoadMaster UI, the **Status** of each Virtual Service is displayed. If the WAF for a particular Virtual Service is misconfigured (for example, if there is an issue with a rule file), the status changes to **WAF Misconfigured** and turns to red.

> If the Virtual Service is in a **WAF Misconfigured** state, all traffic stops flowing. WAF can be disabled for that Virtual Service to stop the traffic being blocked, if required, while troubleshooting the problem.

© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

3 Troubleshooting

Refer to the sections below for some information relating to WAF troubleshooting.

3.1 WAF Logging

All events are logged but there may be a delay in them being available for Administrator viewing. For further information on the WAF logging options, refer to the **WAF Event Log** and **Enable WAF Debug Logging** sections.

3.2 WAF Compatibility with Kerberos Constrained Delegation (KCD)

As of the 7.2.40 LoadMaster firmware version, you cannot enable both WAF and KCD at the same Virtual Service level. For example:

- If WAF is enabled in the parent Virtual Service, you cannot enable KCD as the **Server Authentication Mode** in the parent Virtual Service



- If KCD is enabled in the parent Virtual Service, you cannot enable WAF

However, you can enable ESP/KCD in the SubVS and then enable WAF in the parent Virtual Service.

If you had WAF and KCD enabled at the same level before upgrading to 7.2.40 and you upgrade the firmware to 7.2.40 or above, the configuration will not be changed. File attachments in SharePoint will not work. To resolve this, enable WAF on the parent Virtual Service and ESP/KCD on the SubVS.

The following combination is not supported: WAF with ESP Client Certificate authentication and KCD.

3.3 Unable to Download/Update Daily Updates

Kemp recommends adding the Kemp Licensing Server URLs as allowed URLs on your firewall to ensure all licensing features work, including the downloading and updating of WAF daily updates. The URLs to allow vary depending on your LoadMaster firmware version:

© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

- LoadMaster firmware version 7.2.53 or above (or 7.2.48.3 Long Term Support (LTS) and above): **licensing.kemp.ax**
- LoadMaster firmware versions below 7.2.53 (or below 7.2.48.3 LTS): **alsi.kemptechnologies.com** and **alsi2.kemptechnologies.com**

© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

Appendix A: Legacy Rules

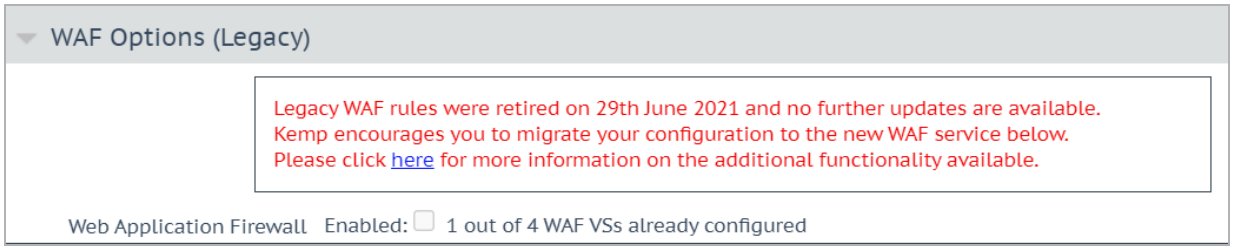
The following sections provide more information about how to configure the legacy WAF rules.

Legacy WAF rules were retired on 29th June 2021 and no further updates are available. Kemp encourages users to migrate their configuration to the new WAF service.

Configure WAF Options (Legacy) for a Virtual Service

WAF settings can be configured for each Virtual Service. Follow the steps below to configure the WAF options (Legacy) in a Virtual Service.

1. In the main menu of the LoadMaster UI, select **Virtual Services > View/Modify Services**.
2. Click **Modify** on the relevant Virtual Service.
3. Expand the **WAF Options (Legacy)** section.



4. By default, WAF is disabled. To enable WAF, select **Enabled**.

   When WAF is enabled for a Virtual Service, the section heading in the Virtual Service options changes from **WAF Options (Legacy)** to **WAF Options (Legacy - Enabled)**

   The maximum number of WAF-enabled Virtual Services is the total (unused or available) RAM (in MB)/512 MB. For example: 8 GB/512 MB = 16 WAF-enabled Virtual Services. When the maximum is reached, no additional Virtual Services can be enabled with WAF.



   A message displays if there is insufficient memory available to enable WAF.

© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

A message is displayed next to the **Enabled** check box showing how many WAF-enabled Virtual Services exist and the maximum number of WAF-enabled Virtual Services that can exist. If the maximum number of WAF-enabled Virtual Services is reached, the **Enabled** check box is greyed out.

5. Specify the **Default Operation** type.

   The **Default Operation** is what occurs if no action is specified in the relevant rule.

   Audit Only: This is an audit-only mode – logs are created, but requests and responses are not blocked.

   Block Mode: Either requests or responses are blocked based on the assigned rules.

6. Specify the **Audit mode**.

   There are three audit modes:
   - **No Audit:** No data is logged.
   - **Audit Relevant:** Logs data that is of a warning level and higher. This is the default option for this setting.
   - **Audit All:** Logs all data through the Virtual Service.

   > Selecting the **Audit All** option produces a large amount of log data. Kemp does not recommend selecting the **Audit All** option for normal operation. However, the **Audit All** option can be useful when troubleshooting a specific problem.

7. Specify whether or not to **Inspect HTTP POST Request Content**.

   The **Inspect HTTP POST Request Content** option is disabled by default. If you enable this option, three more check boxes become available that allow you to enablethe processing of JavaScript Object Notation (JSON), XML requests, and other content types.

8. Enable **Process Responses** to verify response data sent from the Real Servers. .

   The processing of response data can be CPU and memory intensive.

9. Specify the **Hourly Alert Notification Threshold** and click **Set Alert Threshold**.

   This is the number of incidents per hour before sending an alert. Setting this to **0** disables alerts.

10. Assign rulesets by selecting them in the **Available Rulesets** section.

© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

11. Individual rules can be enabled/disabled per ruleset by selecting/clearing them in the box on the right.

    Rules can be filtered by entering a filter term in the **Rule Filter** text box.
    Clicking **Clear All** disables all rules for the selected ruleset.
    Clicking **Set All** enables all rules for the selected ruleset.
    Clicking the **Reset** button disables any rule sets and rules selected since the last time you clicked **Apply**.

12. When finished enabling/disabling the relevant rulesets and rules, click **Apply**.

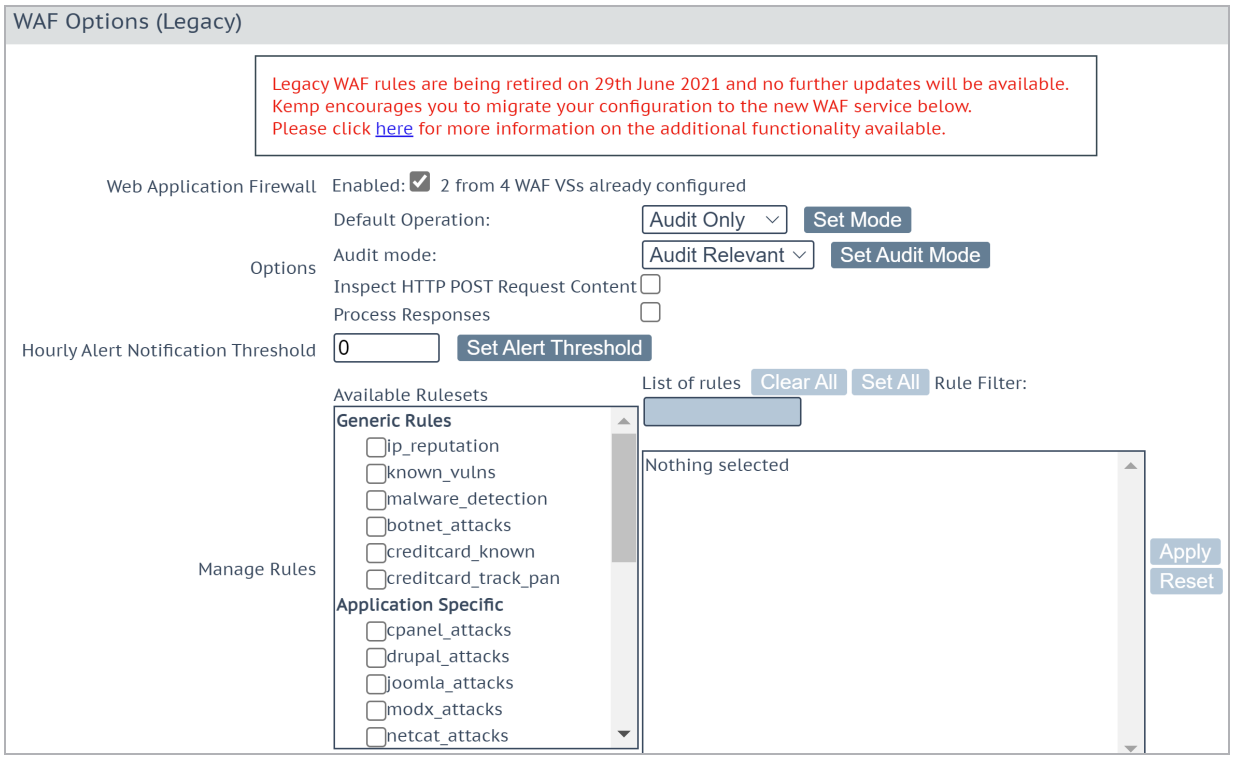
    Application-specific and application-generic rules cannot both be assigned to the same Virtual Service. If you try to do this, an error message (**Cannot assign Application Specific and Application Generic rules simultaneously**) appears to inform you that this is not possible.

WAF Options (Legacy) in the Virtual Service Modify Screen

You can get to the Virtual Service WAF Options by selecting **Virtual Services > View/Modify Services** in the main menu, clicking **Modify** on the relevant Virtual Service and expanding the **WAF Options (Legacy)** section.

By default, WAF is disabled. To enable WAF on this Virtual Service, select the **Enabled** check box. This must be enabled to configure any further options.

© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.



Default Operation

Specify the Default Operation type:

- **Audit Only:** This is an audit-only mode – logs are created, but requests and responses are not blocked. It is recommended when first using WAF to enable **Audit Only** mode for a while. During this time you should analyze the logs and adjust the rules and settings as needed before enabling **Block Mode** . This ensures that no legitimate traffic is blocked.
- **Block Mode:** Either requests or responses are blocked based on the assigned rules.

Audit mode

Audit logs are produced according to the specifications on the following website:
https://github.com/SpiderLabs/ModSecurity/wiki/ModSecurity-2-Data-Formats

Select what logs to record:

- **No Audit:** No data is logged.
- **Audit Relevant:** Logs data which is of a warning level and higher. This is the default option for this setting.
- **Audit All:** Logs all data through the Virtual Service.

© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

> Selecting the **Audit All** option produces a large amount of log data. Kemp does not recommend selecting the **Audit All** option for normal operation. However, the **Audit All** option can be useful when troubleshooting a specific problem.

Inspect HTTP POST Request Content

Enable this option to also process the data supplied in POST requests.

> The **Inspect HTTP POST Request Content** option is disabled by default. If you enable this option, three more check boxes become available that allow you to enable the processing of JavaScript Object Notation (JSON), XML requests, and other content types.

Enable verification of JavaScript Object Notation (JSON) POST requests.

Enable XML Parser

Enable verification of Extensible Markup Language (XML) POST requests.

Enable Other Content Types

Enable verification of POST content types (other than XML/JSON).

> Enabling the inspection of any other content types may increase system resource utilization (CPU and memory). A specific list of content types should be considered.

When the **Enable Other Content Types** option is enabled, there is a text box to enter a comma-separated list of POST content types allowed for WAF analysis. By default, all types (other than XML/JSON) are enabled.

> WAF does not block attack requests if the POST request does not contain the 'content-type' header, even if **Inspect HTTP POST Request Content**, **Enable JSON Parser**, **Enable XML Parser**, and Enable **Other Content Types** check boxes are all enabled. This is a WAF rule issue and can be solved by having a rule to check if there is no 'content-type' present in the request header and forcing the URL-encoded parser in the WAF rules.

© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

Process Responses

Enable this option to verify response data sent from the Real Servers.

> This can be CPU and memory-intensive, so only enable this if necessary.

> If a Real Server is gzip encoding, WAF will not check that traffic, even if **Process Responses** is enabled.

Hourly Alert Notification Threshold

This is the threshold of incidents per hour before sending an alert email. Setting this to **0** disables alerting.

Rules

This is where you can assign/un-assign generic, application-specific, application-generic, and custom rules to and from the Virtual Service.

> You cannot assign application-specific and application-generic rules to the same Virtual Service.

Individual rules within each ruleset can be enabled/disabled as required. To enable a ruleset, select the relevant check box. If you have not enabled/disabled rules in that ruleset previously, all rules are enabled by default in the right box. If you have previously enabled/disabled rules in that ruleset, within that Virtual Service – the rules retain their previous settings.

You can enable/disable individual rules as needed by selecting the relevant ruleset on the left and selecting/clearing the rules on the right.

> Some rules or rule sets may have dependencies on other rules. There is no dependency check in the LoadMaster when rules are disabled - before disabling any rule, be aware of any rule chains or dependencies.

When finished making changes, click **Apply**.

Clicking the **Clear All** button disables all rules for the selected ruleset.

Clicking the **Set All** button enables all rules for the selected ruleset.

Text can be entered in the **Rule Filter** text box to filter the rules to only show rules that contain the filter text.

© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

Clicking **Reset** disables all rulesets and rules.

> Only assign the rules that are required. All assigned rules will be checked against, so a large number of assigned rules can lead to high CPU usage.

© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

References

Unless otherwise specified, the following documents can be found at http://kemptechnologies.com/documentation

Edge Security Pack (ESP), Feature Description

Kemp LoadMaster, Product Overview

Web User Interface (WUI), Configuration Guide

© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

Last Updated Date

This document was last updated on 27 July 2023.

© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.