

LoadMaster 7.2.54.0 Release Notes

Generated on: 16 September 2024

Copyright

Visit the following page online to see Progress Software Corporation's current Product Documentation Copyright Notice/Trademark Legend: Product Documentation Copyright Notice & Trademarks | Progress

Table of Contents

Chapter 1: Introduction 5

Chapter 2: Before You Upgrade (READ ME FIRST). 6

Supported Models for Upgrade 7

Upgrade Path 8

Upgrade Patch XML File Verification Notes 8

Downgrading to Earlier Versions 8

Chapter 3: New Features - WAF Enhancements (WAF 1.5) 9

Native Support for the OWASP Core Rule Set (CRS) 9

Anomaly Scoring and Paranoia Modes 9

Enhanced Log Event Data 10

User Interface Improvements 10

Chapter 4: Change Notices - WAF Rules being retired -- No Further Updates Available. 11

Chapter 5: Issues Resolved. 12

Chapter 6: New Known Issues 14

Chapter 7: Existing Known Issues 15

1

Introduction

LMOS Version 7.2.54.0 is a feature and bug-fix release made available in April 2021. Please read the sections below before installing or upgrading to this GA release.

2

Before You Upgrade (READ ME FIRST)

Please pay special attention to the issues below before you begin an upgrade to this release.

Generation of 4096-bit DHE Key

During an upgrade to this version from a version prior to 7.2.53.0, a new 4096-bit DHE key is generated. On some virtual or hardware appliances, this can lead to significant CPU and memory consumption that could impact regular Virtual Service traffic. Progress Kemp strongly recommends that updates to this release from a version prior to 7.2.53.0 be performed during a maintenance interval.

Best Practices Cipher Set

In 7.2.52.0, the **BestPractices** cipher set was updated. If you are upgrading from a version prior to 7.2.52.0, this change is effective immediately after upgrading to this release. This change was made to improve security and conform to the latest industry best practices.

Note: If you depend on any of the cipher sets being removed from the BestPractices set, then *before you upgrade* you must create a custom cipher set that contains these ciphers and assign this new custom cipher set to the Virtual Services that are currently using the BestPractices cipher set. After this is done, you can upgrade to this release and your services will continue to use the old ciphers. If you do not, then after upgrading, any clients that depend on these ciphers being available will no longer be able to connect.

It is recommended, however, that you migrate your services as soon as possible to use the new **BestPractices** cipher set.

Related Links

- Supported Models for Upgrade
- Upgrade Path

Supported Models for Upgrade

This release of LMOS is supported on the Hardware and Virtual models shown in the first three columns of the table below. *It is not supported and should not be installed on any model listed in the two columns at right.* This update patch can be applied to any supported model regardless of licensing (e.g., SPLA, MELA) or platform (e.g., hardware, local cloud, public cloud).

Supported Virtual Models	Supported Hardware Models	Supported Bare Metal Models	Unsupported Hardware & Virtual Models	Unsupported Virtual Models
VLM-200	LM-X1	LMB-1G	LM-2000	LM-100
VLM-500	LM-X3	LMB-2G	LM-2200	LM-1000
VLM-2000	LM-X15	LMB-5G	LM-2500	
VLM-3000	LM-X25	LMB-10G	LM-2600	
VLM-5000	LM-X40	LMB-MAX	LM-3500	
VLM-10G	LM-2400		LM-3600	
VLM-GEO	LM-3000		LM-5300	
VLM-MAX	LM-3400		LM-5500	
	LM-4000		LM-Exchange	
	LM-5000		LM-GEO	
	LM-5400			
	LM-5600			
	LM-8000			
	LM-8020			
	LM-8020M			
	LM-R320			

If your model number is not listed above, please see the list of End of Life models.

Upgrade Path

You can upgrade to this release of LMOS from any previous 7.2.x release. For full upgrade path information, please see the article Firmware Upgrade Path.

Related Links

- Upgrade Patch XML File Verification Notes
- Downgrading to Earlier Versions

Upgrade Patch XML File Verification Notes

By default, verification of the digital signature on upgrade images is required in LMOS 7.2.50.0 and above. See the **Update Verification Options** setting under **System Administration > Miscellaneous Options > WUI Settings**. If the unit you are upgrading is set to require validation, you'll need to supply the XML Verification File supplied with this release.

Note that:

- In previous releases, *two* verification files were provided: one for pre-7.2.51 systems and one for later systems. This restriction has been removed with the 7.2.53.0 release; if upgrading from firmware 7.2.51.0 / 7.2.48.3 and above you can use the XML file provided with this release. If upgrading from any other firmware version you must following the upgrade path detailed in Kemp LoadMaster Firmware Upgrade Path article.
- LoadMasters running an LMOS version prior to 7.2.49 do not provide the option of XML file verification in the UI or API. If you are upgrading from one of these releases to this release, you can verify the digital signatures offline. For further information, refer to the Verifying XML Signatures Technical Note.

Downgrading to Earlier Versions

Downgrading a LoadMaster running LMOS 7.2.54.0 to LMOS 7.2.51.0 (or a later release) can be performed using any desired **Update Verification Options** setting.

Downgrading to LMOS 7.2.50.0 or a previous release can only be done when the **Update Verification Options** setting is set to **Optional** or **Legacy**. When performing the downgrade, do not specify an XML file. If you want to verify the digital signature on the image before downgrading, you can do so using a Verifying XML Signatures Technical Note.

3

New Features - WAF Enhancements (WAF 1.5)

The following major enhancements to LoadMaster's WAF capabilities are included in LMOS 7.2.54.

Related Links

- Native Support for the OWASP Core Rule Set (CRS)
- Anomaly Scoring and Paranoia Modes
- Enhanced Log Event Data
- User Interface Improvements

Native Support for the OWASP Core Rule Set (CRS)

The OWASP CRS is a set of generic attack detection rules designed to protect web applications from a wide range of attacks, including the OWASP Top Ten. The CRS provides protection against many common attack categories, including SQL Injection, Cross Site Scripting, Local File Inclusion, and others, providing significantly better baseline protection for your applications as well as deeper insight into application traffic attacks.

Anomaly Scoring and Paranoia Modes

Support has been added for utilizing the anomaly scoring and paranoia modes available with the OWASP

CRS to better enable tuning and reducing any false positives.

Enhanced Log Event Data

Additionally, real-time per Virtual Service logging of events and rules triggered whilst performing false positive analysis is available to make WAF operations more transparent to our customers.

User Interface Improvements

The LoadMaster user interface, for WAF, is being significantly modified to allow easy selection of countries to block and this will be reflected in enhanced statistics.

For more information, please see the WAF Feature Description.

4

Change Notices - WAF Rules being retired -- No Further Updates Available

With the introduction of the Open Web Application Security Project® (OWASP) Core Rule Set (CRS) as the primary set of rules-based protection on LoadMaster, the legacy WAF rules are being retired on **29th June 2021**. After this date, you can continue to use the currently installed rules, but *no further updates will be available*. These legacy rules will remain available in the LoadMaster user interface under the title 'WAF Options (Legacy)'.

5

Issues Resolved

PD-18022	**IPv6**: If packet filtering is enabled, returning IPv6 traffic destined for a Real Server acting as a client is ignored by LoadMaster. This issue has been fixed.
PD-17940	**Wildcard VS**: After upgrade to 7.2.53, Loadmaster may reboot if a Wildcard Virtual Service exists and connections are not completed by the client. This bug has been fixed.
PD-17921	**Body Response Content Rules**: Fixed an issue where a body response rule applied to an empty file causes a significant response delay.
PD-17878	**Bandwidth Limiting Statistics**: Fixed an issue that caused incorrect client bandwidth limiting statistics to be displayed.
PD-17721	**SSL Certificate Login**: Fixed issues associated with rejecting certificates with an unknown user error when multiple "Other names" are specified in the certificate.
PD-17717	**WAF**: Addressed issues where a specific custom WAF rule could not be added because of internal dependencies within the standard rule set.
PD-17714	**OIDC**: In previous releases, the minimum allowed value for the Application Secret ID length was 32, which caused issues on some providers. With this release, the minimum value is 1.
PD-17694	**User Interface**: Fixed an issue with rendering the Network Telemetry interface table in some browsers.
PD-17693	**ESP Logging**: In previous releases, Layer 7 User Agent logs were appearing in the messages log file when accessing a Virtual Service using Single Sign On even when Layer 7 Debug Logs were not enabled. This issue has been fixed.

PD-17636	**UDP Virtual Service**: Fixed an issue that caused the system to panic when a UDP port 443 Virtual Service was created.
PD-17616	**CSR Generation**: In previous releases, the T61STRING string type was used for the Common Name field of a Certificate Signing Request (CSR) created by LoadMaster. With this release, LoadMaster uses the UTF8STRING string type for the Common Name.
PD-17612	**Licensing**: Fixed an issue with licensed bandwidth limits where Virtual Services with SubVSs would be prematurely limited.
PD-17504	**SSL**: Fixed an issue that caused SSL handshakes to fail between LoadMaster and a Real Server with certain types of EC certificates.
PD-17308	**Body Response Content Rules**: If a user adds a body response rule to a Nested/Cascaded Virtual Service the LoadMaster removes all "Set-Cookie" headers. This bug has been fixed.
PD-17207	**API**: Using the killsession API to end an SSO session results in an overflow error. This issue has been fixed.
PD-16707	**SSO**: **Steering Groups**: Fixed an issue where a user would close the browser and get an error logging into the application again using a steering group.
PD-16495	**GEO**: Fixed an issue where adding an IP address of 0.0.0.0 to an FQDN caused issues. Now, 0.0.0.0 is blocked from being added to an FQDN.
PD-16113	**GEO**: LoadMaster adds the Global TTL to TXT records when local settings are enabled on the FQDN. This issue has been fixed; now, the Local TTL is added when local settings are enabled.
PD-15396	**GEO**: Fixed an issue that caused LM to send a spurious "KEMP GEO" TXT record in DNS responses, if the TXT record field is empty and the queried FQDN is not a sub-domain of the ZoneName.

6

New Known Issues

PD-18467	**Mobile ActiveSync User Single Sign On**: Mobile Devices using ActiveSync are denied access when using Principal Name (e.g., *name*@company.com) to log in. The workaround is to use Username instead (e.g., company*name*).
PD-18099	**Client Certificates**: Authentication may be denied if multiple "Other names" are present in the client certificate.
PD-18028	**Client Certificates**: Under certain circumstances, a user with a valid certificate is incorrectly denied access; adding the email address of the user to the CN field causes login to succeed.
PD-18021	**Content Rule UI**: Display is incorrect when the 'Ignore case' option is enabled.
PD-17934	**Client Limiting**: An internal error can cause client limiting to be incorrectly applied; e.g., log messages may indicate that limiting is being applied, removed, and applied again within a period of time that is shorter than the period set by the user.
PD-17933	**ESP:** When ESP sends data, it sets the Set-Cookie header without a samesite parameter, which causes some browsers to interpret this as "samesite=lax" and possibly refuse to deliver content.
PD-17927	**LDAP UI Access**: Under certain circumstances, a user that has no LDAP credentials can gain access to the UI.
PD-17867	**Historical Graphs**: Under certain circumstances, graphs for VLANs and Bonded Interfaces may no longer appear in the UI after upgrade to 7.2.53.
PD-16140	**GEO Clustering Mode**: TXT records are blank after 1024 IP addresses are added to an FQDN.

7

Existing Known Issues

The following issues appeared in the *Release Notes* for the previous release of LMOS.

PD-15872	**LDAP/Syslog**: StartTLS is not working when the **Server Certificate Validation** flag is enabled.
PD-15633	**GEO**: If you add a Zone Name to GEO *after* you have created working FQDNs, GEO may no longer respond to queries for one or more of the FQDNs after the Zone Name is added. The workaround is to remove and then re-add the FQDNs that are no longer working.
PD-15475	**VS Redirects**: If you attempt to upload a new redirect error HTML file to a Virtual Service with **Not Available Redirection Handling** enabled *while traffic is currently being redirected*, then traffic to the VS is dropped. Click the **Error Message** radio button in the UI and the VS begins accepting connections again.
PD-15354	**SSO Timeout**: In LMOS 7.2.51.0, a fix was introduced for issues that caused an SSO client to not be properly logged out when the configured session timeout expires. It has been observed that while sessions do timeout, they are not always closed immediately upon the expiry of the timer; it can take close to a minute longer for the session to be closed.
PD-15294	**ESP Verify Bearer Header**: LoadMaster does not return an error when an encrypted token is received and there is no SSL certificate assigned to the VS to decrypt the token.
PD-15172	**ESP Verify Bearer Header**: Validation is not working when "Allowed Virtual Hosts" and "Allowed Virtual Directories" are blank on the Virtual Service.
PD-14943	**Single Sign On**: When Form Based Authentication is enabled on the server side, it is possible that after filling out correct credentials and submitting the login form, the form will be presented again; once the second login form is submitted with correct credentials, the login succeeds.

PD-13899	**ACLs and Real Servers**: Real Servers located on networks on which LoadMaster also has an IP address are *always* allowed to access Virtual Services on that network interface regardless of any access control list (ACL) settings on LoadMaster. For Layer 7 services, this issue can be worked around using Content Rules. The workaround for other services is to block access for local Real Servers (if desired) on another network device (firewall, switch, router, etc.).
PD-12838	**ESP / SSO**: The ESP **Permitted Group SID(s)** setting is not working as expected when configured on a SubVS.
PD-12616	**WAF / Compression**: With Web Application Firewall (WAF) enabled, compressed files are incorrectly decompressed. As a workaround, ensure compression is enabled in VS Advanced Properties by selecting the **Enable Compression** option.
PD-12492	**Downgrade**: If an **Azure VLM** is downgraded to the LTS firmware release (7.1.35.x), the WUI may display in the top right-hand corner that the VLM is a **Hyper-V VLM**. This indicates that the **Azure VLM Add-On Package** must be added to the system to provide full Azure VLM functionality. If this occurs, please contact Kemp Support to get the required add-on package.
PD-12354, PD-10466	**Hardware Support**: The LoadMaster models LM-X15, LM-X25, and LM-X40 do not support the following SFP+ modules: LM-SFP-SX (SFP+ SX Transceiver 1000BASE-SX 850nm, 550m over MMF), LM-SFP-LX (SFP+ LX Transceiver 1000BASE-LX 1310nm, 10KM over SMF).
PD-12237	**HA / NTP**: Configuring NTP for the first time *after* the system is running in High Availability (HA) mode *and* when the current time on the machines is not correct, may cause the systems to both go into the Master state.
PD-12147	**ESP / RADIUS**: In a LoadMaster configuration with ESP and Radius server-side authentication enabled, sessions may fail to be established.
PD-12058	**Browser Support**: An issue exists when connecting to the LoadMaster WUI when using newer versions of the Firefox browser on initial configuration of a hardware FIPS LoadMaster.
PD-11861	**RADIUS / IPv6**: IPv6 is not supported by the current RADIUS implementation in the LoadMaster for both WUI Authorization and ESP Authentication.
PD-11166	**Networking**: Azure LoadMasters are not translating the additional network address between the Master and Slave correctly.
PD-11044	**SharePoint Virtual Services**: A second authentication prompt is presented when a file is uploaded to SharePoint with the following configuration: WAF is configured with **Process Responses** enabled on the main Virtual Service and KCD is enabled on the SubVS level for server-side authentication.
PD-10917	**HA**: An issue exists when setting up a 2-armed HA Virtual LoadMaster in Azure.
PD-10784	**HA**: Configuring LoadMaster HA using eth1 on an Amazon Web Services (AWS) Virtual LoadMaster does not work.
PD-10586	**GEO**: If a GEO FQDN is configured with **All Available** as the **Selection Criteria**, IP addresses are returned even if the cluster is disabled.
PD-10490	**Content Rules**: The *vsremovewafrule* RESTful API command does not allow multiple rules to be removed.
PD-104	**Intrusion Detection**: A SNORT rule is triggering a false positive in certain scenarios.

74	
PD-10193	**Exchange 2010 Virtual Services**: A WAF, ESP, and KCD configuration with Microsoft Exchange 2010 is not supported.
PD-10188	**Browser Support**: (Safari) When adding a Real Server to a Virtual Service or SubVS using the Safari browser, the list of available Real Servers is not available.
PD-10159	**Statistics**: When upgrading firmware from version 7.1.35.*n*, CPU and network usage graphs are not appearing. As a workaround, reset the statistics in the WUI.
PD-10136	**Clustering**: In a LoadMaster cluster configuration, a new node can be added with the same IP address as an existing node.
PD-9816, PD-9476	**WAF**: There is an API command to list individual rules in a ruleset, but there is no command to list the available rulesets themselves.
PD-9765	**GEO**: DNS TCP requests from unknown sources are not supported.
PD-9507	**Networking**: Unable to add an SDN controller using the RESTful API/WUI in a specific scenario.
PD-9375	**SharePoint Virtual Services**: Microsoft Office files in SharePoint do not work in Firefox and Chrome when using SAML authentication.