

LoadMaster 7.2.48.4 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

Best Practices Cipher Set 6

Chapter 3: Supported Models for Upgrade 7

Chapter 4: Upgrade Path 9

Upgrade Patch XML File Verification Notes 9

Chapter 5: New Features 10

Network Telemetry 10

Chapter 6: Change Notices 12

LoadMaster Licensing FQDN Change 12

Chapter 7: Security Updates 13

NTLM Proxy Mode 13

Chapter 8: Issues Resolved. 14

Chapter 9: Existing Known Issues 16

1

Introduction

LMOS Version 7.2.48.4 is a feature and bug-fix update release for the LMOS Long Term Support (LTS) version 7.2.48, made available in March 2021. Please read the sections below before installing or upgrading.

2

Before You Upgrade (READ ME FIRST)

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

Related Links

- Best Practices Cipher Set

Best Practices Cipher Set

In LMOS 7.2.48.3, the **BestPractices** cipher set was updated. If you are upgrading from a version prior to 7.2.48.3, this change is effective immediately after upgrade to this release. This change was made to improve LoadMaster 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 upgrade 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.

3

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**	

Supported Virtual Models	Supported Hardware Models	Supported Bare Metal Models	Unsupported Hardware & Virtual Models	Unsupported Virtual Models
	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.

4

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

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.

5

New Features

Refer to the following sections for details on the new features in this release.

Related Links

- Network Telemetry

Network Telemetry

LMOS expands the value it provides to customers with native support for export of Network Telemetry data to external collection and analysis devices – such as **Kemp Flowmon Collector**.

It does this by combining the power of the data available to LoadMaster (by virtue of being a key link in the application delivery chain) with the power of the Kemp Flowmon Probe's ability to compile and export **NetFlow/IPFIX** telemetry data.

- The **Kemp Flowmon Probe** aggregates network metadata natively on LoadMaster, enabling lightweight, yet incredibly detailed, network and application monitoring when interpreted by a NetFlow/IPFIX collector, such as the **Kemp Flowmon Collector**.
- The **Collector** then stores, processes, and analyzes the flow data and enables comprehensive network monitoring, diagnostics, and troubleshooting, as well as zero-day threat and anomaly detection. Collector is completely customizable through its modular approach to analytic technology; you can choose the mix of Collector module that suit your deployment and data analysis goals.

In addition, a Dashboard Installer Script is provided that uses the Flowmon Collector RESTful API to create LoadMaster-specific dashboards that you can use as-is or modify to suit your needs.

Click **Network Telemetry** in the LoadMaster UI's main menu to download a demo of the Flowmon Collector and configure LoadMaster to export IPFIX protocol data to the Collector.

6

Change Notices

Refer to the following sections for change notices relating to this release.

Related Links

- LoadMaster Licensing FQDN Change

LoadMaster Licensing FQDN Change

The LoadMaster licensing Fully Qualified Domain Name (FQDN) has changed. Previously, the FQDN was alsi.kemptechnologies.com. Now, it is licensing.kemp.ax. In some scenarios, Kemp recommends adding the licensing FQDN as an allowed URL on your firewall to ensure all licensing features work, including the downloading and updating of Web Application Firewall (WAF) rules. The URLs to allow vary depending on your LoadMaster firmware version:

- LoadMaster firmware version 7.2.48.3 and above: **licensing.kemp.ax**
- LoadMaster firmware versions below 7.2.48.3: **alsi.kemptechnologies.com** and **alsi2.kemptechnologies.com**

7

Security Updates

Refer to the following section for security updates relating to this release.

Related Links

- NTLM Proxy Mode

NTLM Proxy Mode

A new **NTLM Proxy Mode** option has been added that changes the behavior of NTLM to utilize the Real Server as a proxy for NTLM authentication validation, improving the security of the overall deployment.

After upgrade to this release, turn on **NTLM Proxy Mode** by doing the following:

1. In the main menu, go to **System Configuration > Miscellaneous Options > L7 Configuration**.
2. Enable the **NTLM Proxy Mode** check box. This changes the **NTLM** selection for **Client Authentication Mode** in all Virtual Services to **NTLM-Proxy**.

NTLM Proxy Mode is enabled by default for all new deployments of LMOS 7.2.53.0 (and above), as well as the LTS release branch (7.2.48.4 and above).

8

Issues Resolved

PD-17616	**SSL Certificate Signing Request (CSR)**: In previous releases, a CSR generated on the LoadMaster uses a type of T61STRING for the Common Name. LoadMaster has been modified to use a type of UTF8String to conform with RFC5280.
PD-17606	**UI SSL Certificate (Azure Only)**: In previous releases, for the Azure cloud only, the LoadMaster UI's SSL Certificate SAN (Subject Alternative Name) information was missing several fields: the LoadMaster Public IP Address, the DNS IP Address, and the Azure-LB IP Address (if applicable). These fields are now added to the Azure cloud LoadMaster UI certificate.
PD-17518	**User Login Certificates**: In previous releases, user certificates generated when adding a user with the "No Local Password" option enabled didn't contain any "Extended Key Usage" information. This issue has been fixed.
PD-16960	**Logging / Security**: Fixed a bug where the LoadMaster **syslog** server wasn't honoring the **Outbound Connection Cipher Set** setting when originating connections to a remote server.
PD-16937	**Layer 7 (Chunked Content)**: When a Real Server returns chunked content, the LoadMaster can hang when processing the response and also experience memory exhaustion when under very high load. In adiition, responses to client may also be complressed even if compression is not configured. Content-length header can also be incorrect if server response is chunked, above 954 MB, and body rules are in use. This issue has ben addressed so that LoadMaster no longer hangs and runs out of memory; doesn't compress content when not configured; and, the content-length header is correct for large responses.
PD-16812	**Authentication (LDAPS)**: Fixed an issue that caused LDAPS debug information to be displayed when a client certificate without email information is presented for UI authentication.
PD-16513	**UI Authentication via LDAPS**: Fixed a bug where LDAPS was not checking "Basic Constraints" as required for intermediate certs in a chain.

PD-16361	**SSL Certificates**: LoadMaster has been modified to reject an otherwise valid server certificate that lacks the Server Authentication purpose in the extendedKeyUsage field; no connection is established in this case.
PD-16342	**Layer 7 POST Handling**: Addressed various issues related to POST handling capabilities and error detection within L7, in particular with large POSTs and 401 responses from LoadMaster.

9

Existing Known Issues

PD-19496	**Stability**: In rare cases, an unexpected reboot may occur as the system is stopping a Virtual Service (because, for example, there are no Real Servers available). If a new connection to the Virtual Service is received during a very short period of time during the process of stopping the Virtual Service, then the system may reboot.
PD-19272	**Platform Support**: Fresh deployments of this release to Open Telekom Cloud set the UI port incorrectly to port 443 (instead of 8443, as documented). The workaround is to reconfigure the OpenCloud TCP security rules to use port 443 instead of 8443, and then access the UI using port 443.
PD-13904	**SSO**: Password expiry notifications do not currently work with Forms Based Authentication (FBA) enabled on the server side.
PD-13873	**10 Gb Interfaces (AWS only)**: The AWS driver for 10 Gb interfaces (ENA) does not provide a link indication in its output, and so 'No Link' is the status displayed for a 10 Gb interface on AWS. Interface graphs for 10 Gb interfaces on the statistics page are not scaled properly, and so can run off the display; this will be addressed in a future release.
PD-13385	**WAF**: With WAF enabled on a Virtual Service, HTTP PUT commands that use chunked transfer encoding are dropped. This issue will be fixed in a future release.
PD-12838	**ESP / SSO**: The ESP **Permitted Group SID(s)** setting is not working as expected when configured on a SubVS.
PD-12653	**Networking**: A Hyper-V VLM won't boot when a 4th NIC is added.
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	**Hardware Support**: The LoadMasters LM-X25 and LM-X40 do not support the following SFP+ modules in this release: 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-10474	**Intrusion Detection**: A SNORT rule is triggering a false positive in certain scenarios.
PD-10466	**Hardware Support**: The LoadMaster LM-X15 does not support the following SFP+ modules in this release: 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-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-10129	**Virtual Services**: There is a discrepancy in validation between global-level connection timeout and Virtual Service-level timeout.
PD-9854, PD-13385	**WAF**: When WAF is enabled, any requests received that have chunked transfer encoding enabled (e.g., POSTs) are not processed properly and are not forwarded to a real server.
PD-9816	**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-9476	**WAF**: There is no RESTful API command to get/list the installed custom rule data files.
PD-9375	**SharePoint Virtual Services**: Microsoft Office files in SharePoint do not work in Firefox and Chrome when using SAML authentication.
PD-8853	**GEO**: **Location Based** failover does not work as expected.
PD-8725	**GEO**: **Proximity** and **Location Based** scheduling do not work with IPv6 source addresses.