

LoadMaster 7.2.48.5 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 VLAN Enhancement 10

Chapter 6: Change Notices 12

"Allow Access on Server Fail" Now Applies to SSO 12

Certificate Signing Request (CSR) Generation Permissions 13

AWS: Downgrade from LMOS 7.2.55.0 13

Chapter 7: Security Updates 14

Unblocking 'bal' Account After Failed Login 14

Console Support for WUI Cipher Reset 14

Console CLI Security Update 15
WUI Template Security Update 15

Chapter 8: Issues Resolved. 16

Chapter 9: Existing Known Issues 18

1

Introduction

LMOS Version 7.2.48.5 is a feature and bug-fix update release for the LMOS Long Term Support (LTS) version 7.2.48, made available on 27 October 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 VLAN Enhancement

Network Telemetry VLAN Enhancement

In previous releases, Network Telemetry could not be enabled on a VLAN with an IP address if the underlying interface was not also assigned an IP address. In this release, Network Telemetry can be enabled on a VLAN regardless of whether the underlying interface has an IP address.

Network Telemetry is an add-on package. After you upgrade to LMOS 7.2.48.5, do one of the following to get the latest package:

- If you're installing Network Telemetry for the first time, navigate to **Network Telemetry** in the LoadMaster main menu and click **Install** to get the latest add-on package.
- If you installed Network Telemetry on an earlier release, then after upgrading to LMOS 7.2.48.5 you can get the latest version of the add-on as follows:
  1. Go to the Other Downloads page on the Kemp website.
  2. Click on the **Network Telemetry Flowmon Add-On** link.
  3. The download page lists the add-on packages for both the latest GA release and for the LTS (Long Term Support) release. Click on the link for the **7.2.48.5** add-on.
  4. Once the download is complete, unzip the archive. There will be two files: the add-on image and an

XML file.

5. Navigate to **System Configuration > System Administration > Software Update** in the LoadMaster UI. The bottom section of the screen should look like this:

   mceclip1.png

6. Click the **Browse** buttons to upload the software package and the XML verification file.
7. Once the files are uploaded, click **Install Addon Package**.
8. Once the package is installed, click **OK** on the confirmation message that appears. The **Version Installed** in the screen above should now be 7.2.48.5.nnnnn.RELEASE.

Note: In a small number of cases, LoadMaster needs to be rebooted to complete the add-on upgrade. If the Flowmon add-on package appears in `red text` in the screen above, a reboot is required. Navigate to **System Configuration > System Administration > Reboot System** and click **Reboot**. Otherwise, the package is ready to use after you install or update it.

6

Change Notices

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

Related Links

- "Allow Access on Server Fail" Now Applies to SSO
- Certificate Signing Request (CSR) Generation Permissions
- AWS: Downgrade from LMOS 7.2.55.0

"Allow Access on Server Fail" Now Applies to SSO

In previous releases, the **Certificates & Security > OCSP Configuration > Allow Access on Server Fail** option applied *only* to OCSP checking of certificate-based authentication via LDAPS *for UI login*. With this release, this option is applied to OCSP checks for *all* LDAPS certificate-based logins managed by LoadMaster, including Single Sign On.

The **Allow Access on Server Fail** option is used to modify LoadMaster's behavior when an OCSP check fails because the server refused the connection or didn't respond. When disabled (the default setting), the behavior is to *disallow* login. When this option is enabled, LoadMaster will allow the login as if the OCSP check passed.

Certificate Signing Request (CSR) Generation Permissions

If **Self-Signed Certificate Handling** is set to **EC certs with an EC signature** (in **Certificates & Security > Remote Access**), CSR generation is restricted to the administrative (**bal**) user only. If **Self-Signed Certificate Handling** is set to a different value, all users can generate CSRs.

AWS: Downgrade from LMOS 7.2.55.0

New deployments of LMOS 7.2.55.0 (and later versions) in the Amazon Web Services (AWS) cloud use the latest AWS Nitro-based machine instances, as described in the 7.2.55.0 Release Notes. Downgrade to an earlier LMOS version was not supported. With the changes made in 7.2.48.5, LoadMasters deployed on an AWS Nitro machine instance can be downgraded to 7.2.48.5 (and later 48.*x* versions).

7

Security Updates

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

Related Links

- Unblocking 'bal' Account After Failed Login
- Console Support for WUI Cipher Reset
- Console CLI Security Update
- WUI Template Security Update

Unblocking 'bal' Account After Failed Login

In previous releases, if the 'bal' account became locked (for example, after too many failed login attempts), the user would have to wait at least 10 minutes before login could be attempted again. With this release, the account can be unlocked immediately using the system console / CLI. After logging into the console, use the menu to navigate to **Local Administration > Web Address > Unblock Admin WUI access** to unblock the 'bal' account.

Console Support for WUI Cipher Reset

The system console has been enhanced to support resetting the cipher set used by the LoadMaster UI, for use cases where setting a cipher set improperly may cause the UI to be unreachable. To use this facility:

1. Log into the system console using the hardware or hypervisor console capability, or via SSH.
2. At the **LoadMaster Configuration** menu, select **Local Administration > Web Address > Restore Admin WUI access to default mode**.

This command does the following:

- Resets the **Certificates & Security > Admin WUI Access > WUI Cipher Set** parameter to the default WUI cipher set.
- Resets the **Certificates & Security > Remote Access > Self-signed Certificate Handling** parameter to the default (RSA self-signed certs).

Console CLI Security Update

The system console has been updated to close vulnerabilities present in the CLI in previous releases that could allow an already authenticated user to obtain a privileged shell. The CVE identifier for this vulnerability is CVE-2021-41068.

WUI Template Security Update

Validation has been enhanced for the upload of a Virtual Service Template to the system, to close a security vulnerability wherein a carefully constructed file can be uploaded as a template and create unwanted files on the filesystem. The CVE identifier for this vulnerability is CVE-2021-41069.

8

Issues Resolved

PD-19272	**Platform Support**: Fresh deployments of earlier releases to Open Telekom Cloud set the UI port incorrectly to port 443 (instead of 8443, as documented). This issue has been fixed so that the UI port is set correctly to port 8443.
PD-19186	**Layer 7: Real Servers Are Local**: Fixed an issue where the **Real Servers Are Local** option was not having the desired effect for a Layer 7 HTTP virtual service that had no content rules.
PD-19006	**ESP Post-Pass Authentication**: Fixed a bug that broke the "Post-Pass" authentication method (and hence broke preauthentication for Citrix Workspace App deployments).
PD-18756	**HTTP/2 Performance**: Fixed issues related to clients that are accepting data slower than real servers are sending data that could negatively affect HTTP/2 performance.
PD-18711	**HTTPS Virtual Services**: In previous releases, users become unable to connect to an HTTPS Virtual Service and messages like this appear in the LoadMaster log: "kernel: L7: Error binding socket -98.". This issue has been fixed.
PD-18042	**SSL**: Fixed an issue that caused SSL handshakes to fail between LoadMaster and a Real Server with certain types of EC certificates.
PD-18030	**Historical Graphs UI**: Addressed an issue that caused some graphs to disappear from the page following upgrade to v7.2.53.
PD-17989	**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-17974	**Body Response Content Rules**: Fixed an issue where a body response rule applied to an empty file causes a significant response delay.

PD-17928	**WUI Login**: In previous releases, certificate based login will fail unless the CN (Common Name) in the certificate includes an *emailAddress* attribute. This bug has been fixed.
PD-17927	**LDAP UI Access**: Fixed an issue that could allow an invalid user to get UI access.
PD-17700	**Network Telemetry**: Modified the UI so that an interface cannot be enabled unless a Collector Endpoint IP adress has been specified.
PD-17390	**IPv6 Support**: Fixed an issue that caused IPv6 services to stop responding after a adding a Virtual Service to the configuration; making another change causes the services to respond again. The way in which IPv6 interface state is managed on VS creation was updated to prevent this issue from occurring.
PD-17325	**Port Following**: Fixed an issue that caused port following to break for a Real Server that is not defined within the virtual service being accessed.
PD-15619	**TLS Handshake**: For some applications (e.g., IOS Mail App or Android 10 Skype App), LoadMaster does not properly downgrade the TLS version used when TLS 1.3 is requested but is not configured on the Virtual Service. This bug has been fixed.

9

Existing Known Issues

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

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-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.