

LoadMaster 7.2.48.3 Release Notes

Generated on: 18 December 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

Chapter 3: Supported Models for Upgrade 7

Chapter 4: Update Image Verification 9

Chapter 5: Change Notices 11

Best Practices Cipher Set Updated 11

Cavium III SSL Accelerator Performance Switch 12

IRQ Pinning Default for LoadMaster MT VNFs 12

Modified Supported Elliptical Curves in LoadMaster Client Hello 13

Chapter 6: Security Updates 14

Best Practices Cipher Set Updated 14

Syslog and LDAPS Server Certificate Validity Checking 15

Enhanced Server-Side KCD Authentication Cipher Option 15

Enhanced NTP Key Exchange Algorithms 15

Regeneration of SSH Host Key 15

Certificate Signing Request (CSR) Generation Permissions 16

Certificate Signing Request (CSR) Generation Key Display 16
X.509 Certificate Format Updated 16
Outbound Connection Certificate Validation 16

Chapter 7: Issues Resolved 18

Chapter 8: Existing Known Issues 20

1

Introduction

LMOS Version 7.2.48.3 is a feature and bug-fix release made available in December 2020. Please read the sections below before installing or upgrading.

2

Before You Upgrade (READ ME FIRST)

This release updates the **BestPractices** cipher set as shown in the section below and this change is effective immediately after upgrade to this release. This change is being made to improve LoadMaster security and conform to the latest industry best practices. For more information on the cipher suites being removed from the set, please see the section Best Practices Cipher Set Updated, below.

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 to the Virtual Services that are currently using the **BestPractices** cipher set. If you do not, any clients that depend on these ciphers being available will no longer be able to connect. After this is done, you can upgrade to LMOS 7.2.48.3 and your services will continue to use the old ciphers.

It is recommended, however, that you migrate your services as soon as possible to use the new **BestPractices** cipher set provided with LMOS 7.2.48.3.

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

Update Image Verification

Depending on the LMOS version running on the LoadMaster you are updating, you may need to supply one of the XML verification files when upgrading. See the notes for your release below.

Currently Running Version	Update Notes
7.2.51 *or later*	Verification of the digital signature on update images is required by default. See the **Update Verification Options** setting under **System Administration > Miscellaneous Options > WUI Settings**. If the unit you are updating is set to require validation, you *must* upload the following XML Verification file supplied with this release during the update process: **7.2.48.3.19710.RELEASE.PATCH-64-MULTICORE.checksum.xml** After the update, any capabilities specific to 7.2.51 will no longer be available on LoadMaster.
7.2.50	Same as above, except a different XML file supplied with this release *must* be uploaded during the update process: **7.2.48.3.19710.RELEASE.PATCH-64-MULTICORE-pre7.2.51.0.checksum.xml** After the update, any capabilities specific to 7.2.50 will no longer be available on LoadMaster.

Currently Running Version	Update Notes
7.2.49.1	Online verification not supported. You can verify the digital signature using a Verifying XML Signatures Technical Note using the same verification file as shown above for 7.2.50. After the update, any capabilities specific to 7.2.49.1 will no longer be available on LoadMaster.
7.2.48.2 *or earlier*	Online verification not supported. You can verify the digital signature using a Verifying XML Signatures Technical Note using the same verification file as shown above for 7.2.50.

If you are currently running LMOS 7.1.x or an earlier version, please see the article LoadMaster Firmware Upgrade Path for full upgrade path information.

5

Change Notices

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

Related Links

For details, see the following topics:

- Best Practices Cipher Set Updated
- Cavium III SSL Accelerator Performance Switch
- IRQ Pinning Default for LoadMaster MT VNFs
- Modified Supported Elliptical Curves in LoadMaster Client Hello

Best Practices Cipher Set Updated

In LoadMaster firmware version 7.2.52, the **BestPractices** cipher set was updated. The cipher set is now based on the recommendations provided in the **Use Secure Cipher Suites** section of the following SSL Labs article: SSL and TLS Deployment Best Practices. The following table shows the ciphers that remain in the **BestPractices** cipher in LMOS 7.2.52 in the left column, and the ciphers removed from the set in the right column:

Carried Forward	Removed
ECDHE-ECDSA-AES256-GCM-SHA384	DHE-RSA-AES256-GCM-SHA384

Carried Forward	Removed
ECDHE-RSA-AES256-GCM-SHA384	DHE-DSS-AES256-GCM-SHA384
ECDHE-RSA-AES256-SHA384	DHE-RSA-AES256-SHA256
ECDHE-ECDSA-AES256-SHA384	DHE-DSS-AES256-SHA
ECDHE-RSA-AES128-GCM-SHA256	DHE-RSA-AES256-SHA
ECDHE-ECDSA-AES128-GCM-SHA256	DHE-RSA-AES128-GCM-SHA256
ECDHE-RSA-AES128-SHA256	DHE-DSS-AES128-GCM-SHA256
ECDHE-ECDSA-AES128-SHA256	DHE-RSA-AES128-SHA256
	DHE-RSA-AES128-SHA
	DHE-DSS-AES128-SHA256
	ECDHE-RSA-AES256-SHA
	ECDHE-ECDSA-AES256-SHA
	ECDHE-RSA-AES128-SHA
	ECDHE-ECDSA-AES128-SHA

In addition to the above, the following two ciphers were *added* to the **BestPractices** set:

ECDHE-ECDSA-CHACHA20-POLY1305

ECDHE-RSA-CHACHA20-POLY1305

Cavium III SSL Accelerator Performance Switch

Customers with LoadMaster hardware (e.g., an LM-X40) with a Cavium III hardware SSL accelerator installed have reported performance issues when using the Cavium III hardware with TLS 1.3. A new switch has been introduced on the **Network Options** page in the UI that allows you to switch from using the current 1.1.1 OpenSSL libraries to using the older 1.0.2 libraries, which do not exhibit the performance issues seen with the 1.1.1 libraries; please note, however, that the older libraries do not support TLS 1.3. Please consult with Kemp Support before enabling this workaround. [Note that these performance issues do not apply to Cavium V hardware.]

IRQ Pinning Default for LoadMaster MT VNFs

When using this or a subsequent release as a VNF node in a LoadMaster Multi-Tenant (MT) deployment, the IRQ Pinning option on LoadMaster is now enabled by default when the VNF is deployed to improve overall system performance.

Modified Supported Elliptical Curves in LoadMaster Client Hello

In previous releases, the LoadMaster proposed the following Elliptical Curves for ECDHE ciphers in the client hello:

- secp256r1
- secp384r1
- secp521r1
- x25519
- x448

The last two curves (x25519 and x448) are no longer supported to meet Common Criteria security requirements.

6

Security Updates

The following changes to existing LMOS features and behavior have been made in this release to improve LoadMaster's security profile.

Related Links

For details, see the following topics:

- Best Practices Cipher Set Updated
- Syslog and LDAPS Server Certificate Validity Checking
- Enhanced Server-Side KCD Authentication Cipher Option
- Enhanced NTP Key Exchange Algorithms
- Regeneration of SSH Host Key
- Certificate Signing Request (CSR) Generation Permissions
- Certificate Signing Request (CSR) Generation Key Display
- X.509 Certificate Format Updated
- Outbound Connection Certificate Validation

Best Practices Cipher Set Updated

See the Best Practices Cipher Set Updated.

Syslog and LDAPS Server Certificate Validity Checking

LoadMaster has been modified to use OCSP to check the validity of the server certificates supplied by syslog and LDAPS servers configured into the configuration. If these checks fail, connections to the server are not permitted.

Enhanced Server-Side KCD Authentication Cipher Option

A new option for server-side Kerberos Constrained Delegation (KCD) authentication improves the security of LoadMaster's server side KCD connections to meet evolving security policies.

In previous release, KCD was configured to use RC4, DES, and DES3 ciphers for server connections; these ciphers could not be modified. With this release, you can now enable the **Use AES 256 SHA1 KCD Cipher** option on the **Virtual Services > Manage SSO** UI page to specify that the RC4, DES, and DES3 ciphers be disabled for server-side KCD and that the **aes256-cts-hmac-sha1-96** cipher be used instead. This option can be enabled/disabled as needed within different server-side Single Sign On (SSO) configurations.

Enhanced NTP Key Exchange Algorithms

The **SHA-1** hashing algorithm has been added to the key types supported for NTP on the **System Configuration > System Administration > Date/Time** UI page. Click **Show NTP Authentication Parameters** to display the **NTP Key Type** parameter. Note that, in previous releases, SHA-1 was presented as a choice, but this was actually implementing the legacy SHA (a.k.a. SHA-0) hashing algorithm. This has also been corrected in this release, so that the three key types supported are now: **MD5**, **SHA-1**, and **legacy SHA**.

Regeneration of SSH Host Key

The LoadMaster host key that is used for SSH login can now be regenerated using controls on the system console. Log into the console and choose **Local Administration > Regenerate SSH Host Keys** to regenerate the key. Please note the following:

- When you regenerate the LoadMaster's host key, all current SSH clients will need to be updated with the new public key. Clients will receive connection errors and be unable to connect until the new public key is added to the client's known_hosts file.
- When LoadMaster is configured in either the High Availability or Clustering modes, the host keys on the two LoadMasters are automatically synchronized to maintain the SSH connection on which the configuration depends.
- Note that in GEO Partnering mode, SSH host keys are *not* automatically synchronized, because GEO does not use a shared IP address and the information exchange between partners doesn't depend on

SSH access.

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.

Certificate Signing Request (CSR) Generation Key Display

In previous releases, both the unsigned Certificate Signing Request (CSR) generated by LoadMaster and the associated private key were displayed in the UI (or returned via the API). A new option has been provided to allow the private key to be managed more securely, preventing unintentional disclosure or improper handling of the private key by the user.

This new option appears only when the **Certificates & Security > Remote Access > Self-Signed Certificate Handling** option is set to **EC certs with an EC signature** -- which means that an elliptical curve cipher will be used for both the certificate and the digital signature.

Once the above option is selected, a new **Display Private Key** check box appears on the **Certificates & Security > Generate CSR** UI page.

- When **Display Private Key** is *disabled* (the default), the private key is *not* displayed in the UI after the CSR is created. The unsigned CSR is downloaded by the user as in previous releases. Once it is signed by a Certificate Authority, the user uploads the signed certificate to the LoadMaster -- the difference from previous releases being that the user does not have to also upload the private key, since LoadMaster maintains it internally when **Display Private Key** is disabled. If the saved private key matches the new certificate, the certificate gets imported and the saved private key is deleted. The stored private key is not encrypted but there is no access to it from the outside and it cannot be seen or displayed.
- When **Display Private Key** is *enabled*, LoadMaster behaves as in previous releases: the private key is displayed to the user and must be uploaded to LoadMaster along with the private key.

X.509 Certificate Format Updated

LoadMaster has been enhanced to use the X.509v3 certificate format, as defined in RFC 5280. [Previously, the X.509v1 format defined in RFC 1422 was used.]

Outbound Connection Certificate Validation

Certificate chain validation has been enhanced for all outbound connections:

- The entire certificate chain sent by remote servers is verified back to the trusted signing Certificate Authority (CA).
- For OCSP servers, the certificate must also contain the OCSP Signing purpose (id-kp 9 with OID 1.3.6.1.5.5.7.3.9) in the **extendedKeyUsage** field.

In all cases, the appropriate certificates for chain of trust validation will need to be uploaded to the LoadMaster certificate store.

7

Issues Resolved

The following issues from previous LMOS releases have been addressed in this release.

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-16157	**High Availability (HA) Status**: On the Open Telecom platform only, LoadMasters configured into HA show a status of Active/Active if multiple health checks are being executed and these connections remain open for long periods. This bug has been fixed and HA status is now displayed appropriately.
PD-16156	**LDAP**: Enhanced the UI and API to support the hyphen character (-) in LDAP endpoint names.
PD-16134	**AWS Machine Instances**: On the AWS cloud platform only, LM was observed not to boot properly when using certain newer machine sizes with BIOS versions above Version 9. This issue has been fixed.
PD-16122	**Reliability and Stability**: Fixed an issue with processing large amounts of chunked data from servers with compression enabled that could cause the system to become temporarily unavailable (and a failover to occur in High Availability mode).
PD-16057	**Logging**: In previous releases, various log messages included the file system location of the syslog configuration file. All such messages have been modified to remove the configuration file location.
PD-15869	**Adaptive Health Check Agent**: Updated the adaptive health check mechanism to use HTTP 1.1 (instead of HTTP 1.0) when making Real Server connections.

PD-15860	**Real Server Configuration**: Fixed an issue where the parameter values of a Real Server that has been created with a DNS FQDN (instead of an IP address) cannot be modified.
PD-15828	**Single Sign On (SSO)**: On previous releases, access may be denied during SSO when correct credentials have been supplied, along with log messages indicating "XSS attack dtcode 7". This issue occurs because in some cases LoadMaster is not properly handling SameSite cookie options contained in the client request. This issue has been fixed.
PD-15788, PD-15337	**Login Security**: Fixed a bug that caused two issues: (1) the **Failed Login Attempts** parameter is ignored and users are not getting locked out; and, (2) it is possible under specific circumstances for a user to be logged into another user's current session.
PD-15689	**MELA**: Fixed an issue that caused the LoadMaster MELA Activation Check to fail when LoadMaster contacts Kemp 360 Central.
PD-15578	**NTLM**: In previous releases, when NTLM is enabled on a VS, the LoadMaster reads the request headers, determines that the Authorization header is not present, and sends a 401 reply without waiting for any in-transit client data (such as a POST) to complete. This has been fixed; LoadMaster will now wait for all data before sending a response.
PD-15563	**Base System**: Fixed an issue that caused spurious “kernel: hpet1: lost *x* rtc interrupts” messages to be seen in the logs.
PD-15471	**API**: Modified the **ping**, **ping6**, and **traceroute** APIs to support an FQDN or hostname as input.
PD-15470	**GEO / DNS**: Fixed an issue where the name resolution cache was not being flushed when the configuration was reloaded.
PD-15466	**API**: Fixed an issue with the **getraidinfo** and **getraiddisksinfo** APIs, where the response contained HTML-encoded angle brackets, instead of ASCII-encoded brackets.

8

Existing Known Issues

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

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-124	**Downgrade**: If an **Azure VLM** is downgraded to the LTS firmware release (7.1.35.x), the WUI may display

92	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.