

LoadMaster 7.2.54.7 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 4

Chapter 2: Before You Upgrade (READ ME FIRST). 5

Supported Models for Upgrade 6

Upgrade Path 7

Upgrade Patch XML File Verification Notes 7

Chapter 3: Security Updates - OpenSSL 3.0.8 Support (FIPS Mode ONLY). 8

Chapter 4: Change Notices 10

Non-FIPS OpenSSL Updated to Version 1.1.1u 10

Updating a LoadMaster Running 7.2.54.7 in FIPS Mode 10

Exchange 2016 Running on Windows 2012 Incompatible with FIPS Mode 11

Chapter 5: Issues Resolved. 12

Chapter 6: New Known Issues 14

Chapter 7: Existing Known Issues 15

1

Introduction

LMOS Version 7.2.54.7 is a hardware platform, bug fix, and security update of the LMOS 7.2.54.x Long Term Support Feature (LTSF) branch, made available on 06 December 2023. Please read these release notes before upgrading to this 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 column 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
VLM-200	LM-X25-NG	LMB-1G	LM-2000
VLM-500	LM-X40-NG	LMB-2G	LM-2200
VLM-2000	LM-X40M-NG	LMB-5G	LM-2400
VLM-3000	LM-XHC-25G-NG	LMB-10G	LM-2500
VLM-5000	LM-XHC-40G-NG	LMB-MAX	LM-2600
VLM-10G	LM-XHC-100G-NG		LM-3500
VLM-GEO	LM-X1		LM-3600
VLM-MAX	LM-X3		LM-5000
VLM-SPLA-50	LM-X15		LM-5300
VLM-SPLA-100	LM-X25		LM-5500
VLM-SPLA-500	LM-X40		LM-Exchange
VLM-SPLA-3000	LM-X40M		LM-GEO
VLM-SPLA-GEO	LM XHC 25G		LM-UCS Series
	LM XHC 40G		LM-R320
	LM XHC 100G		LM-5400
	LM-3000		LM-8020-FIPS
	LM-3400		VLM-100
	LM-4000		VLM-1000
	LM-5600		
	LM-8000		

Supported Virtual Models	Supported Hardware Models	Supported Bare Metal Models	Unsupported Hardware & Virtual Models
	LM-8020		
	LM-8020M		

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.

Related Links

- Code Signing Certificate Update

Code Signing Certificate Update

On 27 May 2022, the certificate used to sign LoadMaster release artifacts for LoadMaster LMOS version 7.2.54.4 and prior releases expired. Starting with 7.2.54.5, all LTSF releases will be signed with a new certificate. For details on how this might affect you, please see this Announcement on the Support website.

All LTSF releases after that occur after the above date (LMOS 7.2.54.5 and later) will be digitally signed using a newly obtained code signing certificate.

3

Security Updates - OpenSSL 3.0.8 Support (FIPS Mode ONLY)

Software FIPS mode has been updated with the Progress LoadMaster FIPS Object Module (FOM), based on the OpenSSL Version 3.0.8 FOM, and has been submitted for FIPS 140-2 certification.

Software FIPS mode is entered by clicking **Certificates & Security > Remote Access > Enable Software FIPS Mode** in the UI. [Please note that changing to FIPS mode is a one-way change -- you cannot go back to non-FIPS mode after entering FIPS mode.]

There are several differences between the Progress LoadMaster FOM introduced in LMOS 7.2.54.7 and the FOM used in earlier LoadMaster releases. All these changes ensure that LoadMaster complies with the latest security requirements and guidelines for modern FIPS systems. Please ensure that your configuration and application infrastructure are prepared for these restrictions before you update your FIPS system to this release.

- The Progress LoadMaster FOM operates at OpenSSL Security Level 1, which corresponds to a minimum of 80 bits of security. Any keys, ciphers, etc., offering below 80 bits of security are prohibited. Please specifically note the following:
  - RSA keys 1024 bits long or less are prohibited.
  - DSA and DH keys shorter than 1024 bits and ECC keys shorter than 160 bits are prohibited.
  - All export cipher suites are prohibited.
  - SSL version 2 ciphers are prohibited.
  - Any cipher suite using MD5 for the MAC is prohibited.
  - Signatures using SHA1 and MD5 are prohibited.
- SSL3.0, TLS1.0, and TLS 1.1 ciphers are *not available* as required by the latest FIPS standards. They

cannot be enabled in FIPS mode.

- DSA keys are limited to 2048 bits in FIPS mode.
- The cipher sets in FIPS mode include *only* the following FIPS-compliant TLS 1.2 and TLS 1.3 ciphers:
  - AES128-GCM-SHA256
  - AES128-SHA256
  - AES256-GCM-SHA384
  - AES256-SHA256
  - DHE-DSS-AES128-GCM-SHA256
  - DHE-DSS-AES128-SHA256
  - DHE-DSS-AES256-GCM-SHA384
  - DHE-DSS-AES256-SHA256
  - DHE-RSA-AES128-GCM-SHA256
  - DHE-RSA-AES128-SHA256
  - DHE-RSA-AES256-GCM-SHA384
  - DHE-RSA-AES256-SHA256
  - ECDHE-ECDSA-AES128-GCM-SHA256
  - ECDHE-ECDSA-AES128-SHA256
  - ECDHE-ECDSA-AES256-GCM-SHA384
  - ECDHE-ECDSA-AES256-SHA384
  - ECDHE-RSA-AES128-GCM-SHA256
  - ECDHE-RSA-AES128-GCM-SHA256
  - ECDHE-RSA-AES128-SHA256
  - ECDHE-RSA-AES256-GCM-SHA384
  - ECDHE-RSA-AES256-SHA384
  - TLS_AES_128_GCM_SHA256
  - TLS_AES_256_GCM_SHA384

4

Change Notices

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

Related Links

- Non-FIPS OpenSSL Updated to Version 1.1.1u
- Updating a LoadMaster Running 7.2.54.7 in FIPS Mode
- Exchange 2016 Running on Windows 2012 Incompatible with FIPS Mode

Non-FIPS OpenSSL Updated to Version 1.1.1u

The version of OpenSSL used in the default (i.e., non-FIPS) operating mode has been updated from 1.1.1n to 1.1.1u.

Updating a LoadMaster Running 7.2.54.7 in FIPS Mode

A LoadMaster running LMOS 7.2.54.7 in FIPS mode can only be updated to future LMOS releases that contain the OpenSSL 3 FOM. An attempt to update a LoadMaster running 7.2.54.7 in FIPS mode with an LMOS image from any release that uses the previous version of the OpenSSL FOM (1.0.2) will fail.

This only applies to FIPS mode operation. Systems running in non-FIPS mode can be updated to any

supported release as described in the Kemp LoadMaster Firmware Upgrade Path.

LoadMaster can be returned to the release that was running prior to the update to 7.2.54.7 by switching back to the previously installed partition using the **System Configuration > System Administration > Update Software > Restore Software** button. *Please be sure to take a backup of your system before restoring the previous partition.* This can be used to, for example, help you to repeat on the restored partition any configuration changes you had made while running 7.2.54.7.

Exchange 2016 Running on Windows 2012 Incompatible with FIPS Mode

Older versions of the FIPS product supported secure re-encrypted connections to back-end real servers running Exchange 2016 on a Windows 2012 server. With the move to OpenSSL 3 in this release, re-encryption with this configuration is no longer supported, because the ciphers offered by the FIPS Object Module do not match the ciphers available in the Windows configuration.

5

Issues Resolved

LM-3143	**SSO Logging**: Fixed an issue that caused "No such file or directory" logs being displayed while restarting the SSO management process.
LM-3131	**Azure**: Fixed an issue in Azure deployments where the */var/log/waagent* folder is filled and is not automatically cleared as needed.
LM-3129	**Custom Cipher Sets (FIPS mode)**: In previous releases, upgrading a system in FIPS mode to a version that does not support some of the ciphers configured into a custom cipher set, those ciphers remain available in the custom cipher set *after* upgrade. This issue has been fixed.
LM-3098	**RestAPI restorecert (FIPS mode)**: Fixed an issue that caused the **restorecert** API to fail when restoring certificates from a system in non-FIPS mode to a system in FIPS mode.
LM-2446	**GEO**: Fixed a buffer overflow issue that could cause a system crash and resulting denial of service.
LM-2137	**Health Checking**: Fixed an issue that caused health checks to fail when the associated LDAPS endpoint server is unavailable.
LM-2136	**Single Sign On (SSO)**: Fixed an issue observed on LM-X15 hardware where SSO logins are slow or fail under heavy load.
LM-2135	**Single Sign On (SSO)**: Fixed an issue that could cause a user authenticating via NTLM + KCD to gain access with an invalid domain and password.
LM-2131	**High Availability (HA)**: Fixed stability issues with failover where the passing of control from the currently active unit to the standby unit fails or results in control being re-assumed by the currently active unit when this behavior is not enabled.

LM-2130	**Content Rules**: Fixed issues associated with client certificate headers being erroneously deleted.
LM-2129	**Logging**: Fixed an issue that could cause the kernel log message “Error handling task x x” to appear repeatedly in the system log.
LM-2128	**OIDC/OAUTH**: On Azure, it was observed that an initial OIDC/OAUTH login works correctly, but a second login fails with the error “The reply URL specified in the request does not match the reply URLs configured for the application”. This issue has been fixed.

6

New Known Issues

LM-5339	**Single Sign On (SSO):** When **Failed Login Attempts** is set to **0**, a user logging in using invalid credentials (for example, the wrong password) fails to log in, as expected; however, the login will also be blocked. The workaround is to set **Failed Login Attempts** to a higher value.
LM-5303	**Certificate UI**: A certificate having a Common Name (CN) set to the wildcard character (*) displays unrelated text in the UI. This is a cosmetic issue that affects the UI only.
LM-4898	**PowerShell API**: PS cmdlets related to Lets Encrypt are not working.
LM-3095	**FIPS: OCSP: LDAPS**: LM should not authenticate user from LDAPS server if chain is not complete.
LM-3094	**UI / Templates**: Fixed an issue that causes format breakage in the UI when a non-certificate file is uploaded as an intermediate certificate.

7

Existing Known Issues

LM-4121	**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.
LM-3942	**LDAP UI Access**: Under certain circumstances, a user that has no LDAP credentials can gain access to the UI.
LM-3929	**Content Rule UI**: Display is incorrect when the 'Ignore case' option is enabled.
LM-3789	**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.
LM-2749	**API Keys**: An API key created for a remotely managed user (e.g., RADIUS) will not work unless the remote user ID is also added as a local user on LoadMaster.
LM-1038	**ESP / SSO**: The ESP **Permitted Group SID(s)** setting is not working as expected when configured on a SubVS.
LM-143	**ESP Verify Bearer Header**: Validation is not working when "Allowed Virtual Hosts" and "Allowed Virtual Directories" are blank on the Virtual Service.
LM-136	**Client Certificates**: Authentication may be denied if multiple "Other names" are present in the client certificate.