

LoadMaster 7.2.56.0 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 7

Upgrade Patch XML File Verification Notes 8

Downgrading to Earlier Versions 8

Chapter 3: New Features - TLS 1.3 Cipher Suite Selection 9

Chapter 4: Change Notices 10

SNMPv3 Authentication Updates 10

SSO Domain Configuration Field Character Limit Increased 11

Downgrading on AWS 11

UI Usability Updates 11

Chapter 5: Security Updates - CLI Security Fix (Privilege Escalation) . . . 13

Chapter 6: Issues Resolved. 14

Chapter 7: New Known Issues 17

Chapter 8: Existing Known Issues 18

1

Introduction

LMOS Version 7.2.56.0 is a feature and bug-fix release made available on 8 February 2022. 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 (for example, SPLA, MELA) or platform (for example, 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-2400	
VLM-3000	LM-X25	LMB-10G	LM-2500	
VLM-5000	LM-X40	LMB-MAX	LM-2600	
VLM-10G	LM-X40M		LM-3500	
VLM-GEO	LM XHC Series		LM-3600	
VLM-MAX	LM-3000		LM-5000	
VLM-SPLA-50	LM-3400		LM-5300	
VLM-SPLA-100	LM-4000		LM-5500	
VLM-SPLA-500	LM-5600		LM-Exchange	
VLM-SPLA-3000	LM-8000		LM-GEO	
VLM-SPLA-GEO	LM-8020		LM-UCS Series	
	LM-8020M		LM-R320	
			LM-5400	

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 from any previous 7.2.x release. For full upgrade path information, refer to

the following 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 7.2.55.0 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, refer to the Verifying XML Signatures Technical Note.

3

New Features - TLS 1.3 Cipher Suite Selection

Controls have been added to the Virtual Service UI and API that allow you to select the TLS 1.3 ciphers suites offered by LoadMaster to incoming clients when a TLS 1.3 connection is negotiated. By default, all TLS 1.3 ciphers are selected (as in previous releases). Using the controls, any mix of the 5 ciphers supported by TLS 1.3 can be configured. Note that the controls for selecting TLS 1.3 ciphers are visible in the UI only if TLS 1.3 has been selected.

4

Change Notices

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

Related Links

- SNMPv3 Authentication Updates
- SSO Domain Configuration Field Character Limit Increased
- Downgrading on AWS
- UI Usability Updates

SNMPv3 Authentication Updates

Several enhancements have been made to SNMP Version 3 functionality, to provide better security and separation of controls when configuring the system for for SNMP Version 3 (SNMPv3):

- When the **SNMP V3** check box is enabled, options specific to SNMPv2 are hidden (the values are saved).
- SNMPv3 options now include an optional **Privacy Password**. This optional feature provides a second level of security, in addition to the required **Authentication Password**. To enable it, click the **Enable privacy** check box; the **Privacy Password** text box appears (along with the **Privacy protocol** selection box from previous releases).

SSO Domain Configuration Field Character Limit Increased

The text field character limit for SSO client-side and server-side domain configurations has been increased from 98 to 255 characters. If 256 characters are entered, the UI will reject the entered value as invalid and no change will be made. (These controls are available for each VS by clicking **Virtual Services > Manage SSO > Modify**.)

Downgrading on AWS

Starting with version 7.2.55.0, LMOS can only be deployed on an AWS Nitro-based instance type -- and in 7.2.55.0 could not be downgraded to a release prior to 7.2.55.0. Starting with 7.2.56.0, LMOS running on a Nitro instance can be downgraded to any prior release subsequent to and including 7.2.48.5.

UI Usability Updates

The following changes have been made to the organization and functionality of the LoadMaster UI.

1. The **System Configuration > System Administration > AFE Configuration** page has been removed from the UI, and the several screen elements moved to their own separate pages. You can navigate to the new pages following the click paths below. Most use the same as on the removed page, with the one exception noted below. The click paths below show the new locations:
   - **Virtual Services > Cache Configuration**
   - **Virtual Services > Compression Options**
   - **Certificates and Security > IPS / IDS** (formerly: Intrusion Detection Options)
2. The five SSL related options on the **System Configuration > Miscellaneous Options > Network Options** page have been moved to a new page at **Certificates & Security > SSL Options**.
   - **Enable SSL Renegotiation**
   - **Disable Master Secret Handling**
   - **Size of SSL Diffie-Hellman Key Exchange**
   - **Log SSL errors**
   - **OpenSSL Version**
3. The Virtual Service **WAF** properties UI has been revised to provide:
   - a **Rule Filter** for listing a subset of the rules
   - the ability to **Clear All** and **Set All** rules
   - icons to indicate that rule groups can be expanded to display the individual rules
4. The following utilities have been moved from the **System Configuration > Logging Options > Debug Options** page to a new page at **System Configuration > Troubleshooting**.
   - **Perform Top**
   - **Include Top in Backups**
   - **Display Meminfo**

- **Display Slabinfo**
- **Perform an Ifconfig**
- **Perform a Netstat**
- **Include Netstat in Backups**
- **Netconsole Host**
- **Ping Host**
- **Ping6 Host**
- **Traceroute Host**
- **TCP dump**

5

Security Updates - CLI Security Fix (Privilege Escalation)

On Virtual LoadMaster (VLM) only: In previous releases, a malicious, privileged user, who had already gained access to the CLI, could (through a properly constructed series of commands) obtain unrestricted access to the VLM disk image and thereby obtain a debug password to the running system. This vulnerability has been closed. [CVE-2021-45080]

6

Issues Resolved

PD-19882	**HTTP/2 URL Query Limitation**: Fixed an issue (introduced in LMOS 7.2.55.0) that caused a limit of 4096 characters to be imposed upon the Query section of the URL. This issue has been fixed and there is now no limit on the URL query section.
PD-19822	**User Interface**: When 2 or more network interfaces are configured for High Availability (HA) Mode health checks and 2 or more of the checks have failed, the Home Page may display random text in the status boxes. This bug has been fixed.
PD-19807	**Flowmon Collector Add-On**: Fixed an issue that caused the add-on to fail to autostart after download and installation using the controls on the UI Network Telemetry page.
PD-19801	**Real Time Statistics**: Fixed an issue that caused **Cache Entries** and **Cache Memory** to display very large arbitrary values when multiple services re enabled for caching.
PD-19668	**GEO: Disabled Clusters in UI**: Fixed an issue that caused disabled clusters to be omitted from the UI under specific conditions.
PD-19663	**VLANs in UI**: Fixed an issue that caused VLAN IDs to be corrupted on display.
PD-19661, PD-10586	**GEO: Disabled Clusters**: In previous releases, responses were returned for disabled clusters in certain circumstances. GEO has been modified to no longer return responses for disabled clusters when the cluster is disabled and the "Disabled clusters are unavailable" option is turned on.
PD-19623	**WAF**: Fixed a bug (introduced in 7.2.55) that caused Virtual Services to become unresponsive when WAF remote logging is enabled.

PD-19616	**Log Message Error Level**: In previous releases, the message "kernel: L7: Intercept device not open" was set to the "Error" logging level. Since this message indicates that the WAF engine experienced an unexpected connection close and recovered, the log level has been reduced to 'informational'.
PD-19607	**Debugging**: The ability to set process debug levels for *sshd* has been added to the **System Administration > System Log Files > Debug Options > Enabled Extended Debug > Process Debug** page. Logs appear in the system Warning Message File. These options should not be enabled on a production unit without the instruction and assistance of support.
PD-19584	**Health Checks**: Fixed a bug that caused the server following health check functionality to fail to update the status of the following server when HTTP/1.1 is selected Service the check is taken used http/1.1
PD-19570	**GEO**: Fixed a bug (introduced in LMOS 7.2.55) where restarting GEO results in NXDOMAIN responses being returned intermittently for some FQDNS in cases where the AAAA record for the FQDN should have been returned.
PD-19507, PD-19509	**API**: The ability to get, set, and remove the OCSP port value has been added to both the PowerShell and RESTful APIs.
PD-19502	**OIDC Authentication**: Fixed a bug whereby token validation can be bypassed by under certain circumstances when the browser is refreshed.
PD-19496	**Stability**: Fixed an internal error that caused an unexpected system panic and reboot when Virtual Service connections are dropped as new connection requests are being processed.
PD-19488	**Caching**: Fixed an issue that caused expired cache entries to remain in the cache after the associated Virtual Service is stopped and restarted.
PD-19485	**GEO: Intermittent FQDN Resolution Failures**: Fixed an internal issue that could cause intermittent FQDN resolution failures, with repeated retries resulting in a successful response.
PD-19376	**GEO**: Fixed an issue (introduced in LMOS 7.2.55) that caused Site IPs to be incorrectly marked UP when DNS is restarted.
PD-19360	**Real Servers**: Fixed a bug where adding a Virtual Service (VS) with 1024 Real Servers (RSs) prevents duplicating that VS using the same 1024 RSs.
PD-19226	**GEO Partner Stops Responding After Reboot**: Fixed issues that could cause GEO to stop responding after a reboot, producing a "Cannot create BIND" log message and a segmentation fault. This was due to an internal operation (such as a partner synchronization) occurring immediately after the reboot and before all necessary resources for the attempted operation were available.
PD-19216	**WAF**: Fixed an internal error that caused the log message "Cannot open kernel for [VIP], Child PID exited" to appear and WAF to stop functioning.
PD-19194	**AWS:** It is not possible to downgrade a fresh install of LMOS 7.2.55.0 in the AWS Cloud to a earlier LMOS release. This issue has been fixed.
PD-19180	**GEO**: When GEO is running in Cloud High Availability (HA) Mode, DNS remains running on the standby unit as well as the active unit. This issue has been fixed.
PD-19175	**ESP Logging**: Previously, ESP Logs was printing domain/realm name in domain info at logon and session kill events. Now, ESP user logs prints SSO domain configuration name in domain info instead of domain/realm name.

PD-19168	**ESP Logging**: Previously, L7 "Logged on" event log was missing for successful login via certificate in the ESP user log file. Now, L7 "logged on" event log generated upon successful login via certificate.
PD-19131	**Virtual Services**: Fixed a bug where a Virtual Service (VS) with an Alternate IP Address configured cannot communicate with a Real Server that is not using the same port configured for the VS.
PD-19128	**Real Servers Are Local Option**: In previous releases, if the Real Servers Are Local option is enabled and a Virtual Service is configured for Layer 7, communication with local servers is broken if the VS has no content rules defined. This issue has been fixed.
PD-19118	**HTTP/2 File Access**: Customers reported HTTP/2 failures when accessing files using either a MAC client using Safari or Linux clients using the *curl* command, where the real server reports a broken pipe. The workaround was to disable HTTP/2. This bug has been fixed.
PD-19095	**Content Rule UI**: When you configure a content rule, if the name of the rule is not valid, then the page will refresh and all previous input is lost. This issue is fixed.
PD-18974	**WAF UI**: Removed the password length restrictions on the **Web Application Firewall > Export Logs** page.
PD-18968	**Multi-Tenancy**: The "Reboot on link failure option" functionality does not work when LMOS is used as a VNF in a Multi-Tenancy (MT) configuration and so has been removed from the UI when LMOS 7.2.56.0 is used in an MT configuration.
PD-18830	**Single Sign-On**: Fixed an intermittent internal issue that caused all SSO sessions to be terminated.
PD-18789	**SNMP**: Fixed a bug where no SNMP traps are generated when only **SNMP Trap Sink1** is configured.
PD-18736	**Single Sign-On**: Fixed an internal issue where the cookie domain is being erroneously changed during response processing, leading to a login loop.
PD-18693	**WAF**: Fixed issues that could cause a segmentation fault/reboot when the WAF configuration is modified while traffic is being processed by the WAF engine.
PD-18610	**LDAP**: Fixed an API error where an LDAP endpoint is added despite the failure to set one or more options.
PD-18601	**Statistics**: Some network interfaces are not displayed when there are one or more bonded interfaces. This issue has been fixed.
PD-18470	**HTTP/2**: Fixed a bug that caused cookie persistence to fail with HTTP/2 enabled.
PD-16998	**LDAP UI Login**: Fixed a bug that caused UI authentication to fail group checks.
PD-15859	**L7 Health Checks**: When an AD DS server stops responding to authentication requests causing LDAP health check failures, it's possible that unrelated HTTPS health checks could also fail. This internal issue has been fixed.

7

New Known Issues

PD-20101	**Network Telemetry**: The 7.2.56.0 version of the Network Telemetry Add-on may not function after being enabled on one or more interfaces. Flow data will not be sent to the Flowmon Collector and the following message will appear repeatedly in the system log: flowd: Monitor for interface 0 (pid *xxxxx*) died - exited with status 1 The workaround is to remove the 7.2.56.0 version of the add-on package and install the 7.2.55.0 version, using the controls on the **System Configuration > System Administration > Update Firmware** page. The add-on package can be downloaded from this web page.
PD-19953	**SNMPv2c Walk**: When using SNMP Version 2c, the Walk command may not work, returning no data. The workaround is to enable the SNMPv3 check box in the SNMP configuration and then disable it. The Walk command should then work properly via SNMPv2c.
PD-19704	**GEO Cluster Status**: When adding a Cluster that is unavailable (DOWN) to a Site, the Site may reflect the Cluster's status as available (UP) for a short time before changing to DOWN.

8

Existing Known Issues

PD-19108	**GEO**: Modifying an FQDN entry displays a spurious error on the system console, similar to the one shown below. The FQDN is modified properly.
	
	`<FQDN>:794 Uncaught ReferenceError: disp_addrr_elements is not defined`
	`    at <FQDN>:794`
	`(anonymous) @ <FQDN>:794`

PD-19093	**GEO**: Cannot configure GEO into partnering mode unless there is at least one FQDN already defined.
PD-18646	**Certificate-Based Administrative Login**: Using a certificate that does not have a SAN attribute (i.e., no Principal Name) results in a failed login attempt.
PD-18615	**GEO**: No statistics (queries per second, etc.) are displayed for a site if the FQDN is configured to use the "All Available" Selection Criteria.
PD-18099	**Client Certificates**: Authentication may be denied if multiple "Other names" are present in the client certificate.
PD-17927	**LDAP UI Access**: Under certain circumstances, a user that has no LDAP credentials can gain access to the UI.
PD-15872	**LDAP/Syslog**: StartTLS is not working when the **Server Certificate Validation** flag is enabled.
PD-156	**GEO**: If you add a Zone Name to GEO *after* you have created working FQDNs, GEO may no longer

33	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 two machines is not correct, may cause the systems to both go into the Active state. The workaround for the issue of having two Active LoadMasters in HA is as follows: **1.** Reboot the preferred **Active** LoadMaster in the pair. This unit will remain in Active mode after you

	complete this process. 2. Wait 10 seconds. 3. Reboot the preferred **Standby** LoadMaster in the pair. The 10-second wait allows enough time to pass so that the preferred Standby unit can detect that the other unit is in Active mode and transition to Standby mode.
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-10490	**WAF**: The *vsremovewafrule* RESTful API command does not allow multiple rules to be removed. This problem has been fixed.
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.