

LoadMaster 7.2.55.0 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

Supported Models for Upgrade 7

Upgrade Path 8

Upgrade Patch XML File Verification Notes 8

Downgrading to Earlier Versions 8

Downgrading on AWS 8

Chapter 3: New Features 9

Support for Newer AWS Instance Types 9

WAF: Clearing the False Positive Analysis Counters and Events 10

WAF: Configurable OWASP POST Body Size 11

WAF: Remote Logging TLS Version 11

Network Telemetry VLAN Enhancement 11

LoadMaster Dashboard Installer for Collector (Version 2) 12

GEO: Capacity, Performance, and UI Enhancements 12

Chapter 4: Change Notices 14

SSL Renegotiation Disabled By Default 14

Ciphers Use for Re-encryption 14

Increased Size Limitation for SSO Custom Form Images 15

RPS Limiting UI Removed for Non-Offloaded HTTPS Port 443 VSs 15

Chapter 5: Security Updates 16

Update OpenSSL to Version 1.1.1k 16

Strict Transport Security Header Settings 17

Single Sign On: SameSite and Secure Options 17

Console Support for WUI Cipher Reset 18

Certificate Chain of Trust for UI Authentication 18

Console CLI Security Update 18

WUI Template Security Update 18

Chapter 6: Issues Resolved. 19

Chapter 7: New Known Issues 22

Chapter 8: Existing Known Issues 23

1

Introduction

LMOS Version 7.2.55.0 is a feature and bug-fix release made available on 15 September 2021. 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

For details, see the following topics:

- 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 (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-2400	
VLM-3000	LM-X25	LMB-10G	LM-2500	
VLM-5000	LM-X40	LMB-MAX	LM-2600	
VLM-10G	LM-3000		LM-3500	
VLM-GEO	LM-3400		LM-3600	
VLM-MAX	LM-4000		LM-5000	
	LM-5400		LM-5300	
	LM-5600		LM-5500	
	LM-8000		LM-Exchange	
	LM-8020		LM-GEO	
	LM-8020M		LM-UCS Series	
	LM-R320			

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.

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, you can do so using a Verifying XML Signatures Technical Note.

Downgrading on AWS

LMOS 7.2.55.0 now uses AWS Nitro-based instance types (see below). LMOS running on a Nitro instance *cannot be downgraded to a release prior to LMOS 7.2.55.0*. This issue will be fixed in the next LMOS LTS firmware release.

3

New Features

The following new features have been added to LMOS since the previous release.

Related Links

For details, see the following topics:

- Support for Newer AWS Instance Types
- WAF: Clearing the False Positive Analysis Counters and Events
- WAF: Configurable OWASP POST Body Size
- WAF: Remote Logging TLS Version
- Network Telemetry VLAN Enhancement
- LoadMaster Dashboard Installer for Collector (Version 2)
- GEO: Capacity, Performance, and UI Enhancements

Support for Newer AWS Instance Types

We have upgraded our AWS offerings to support 'Nitro-based' instance types as shown in the table below. The recommended instance type or each offering is listed first in **bold**.

VLM-FREE	VLM-500	VLM-3000
t3a.small	**m5d.large**	**m5d.large**
t3a.medium	m5d.xlarge	m5d.xlarge
t3a.large	m5d.2xlarge	m5d.2xlarge
	m5d.16xlarge	m5d.16xlarge
	c5d.large	c5d.large
	c5d.xlarge	c5d.xlarge
	c5d.2xlarge	c5d.2xlarge
	c5d.4xlarge	c5d.4xlarge
	c5d.9xlarge	c5d.9xlarge
	c5d.18xlarge	c5d.18xlarge
VLM-MAX	**BYOL**	**License Agreement Based (Metered/SPLA)**
m5d.large	**m5d.large**	**m5d.large**
All three offerings support the machine types listed above for VLM-3000, plus the following:		
r5d.large	r5d.large	r5d.large
r5d.xlarge	r5d.xlarge	r5d.xlarge
r5d.2xlarge	r5d.2xlarge	r5d.2xlarge
r5d.4xlarge	r5d.4xlarge	r5d.4xlarge
r5d.8xlarge	r5d.8xlarge	r5d.8xlarge

Note that a fresh install of LoadMaster on AWS using one of the Nitro-based instances above ***cannot be downgraded to an earlier release***. This issue will be fixed in the next LMOS LTS firmware release due in October 2021.

WAF: Clearing the False Positive Analysis Counters and Events

A **Reset FPA Counters** button has been added to the **Web Application Firewall > False Positive Analysis** page (which also clears the events table). If desired, the **Download** button at the top right of the **Latest Events** table can be used to download the current list of events before clearing.

WAF: Configurable OWASP POST Body Size

In previous releases, the maximum **Request Body Size Limit** for a POST body was hard coded to 1048576 bytes (1 MB). This setting is now configurable in the Virtual Service (and SubVS) API and UI settings. The default remains 1048576 bytes, with a supported range of 1024 bytes to 10485760 bytes (10 MB). This setting is available in a WAF-enabled Virtual Service under WAF **Advanced Options**. The **Inspect HTTP POST Request Bodies** option must be enabled before this new control is visible in the UI.

WAF: Remote Logging TLS Version

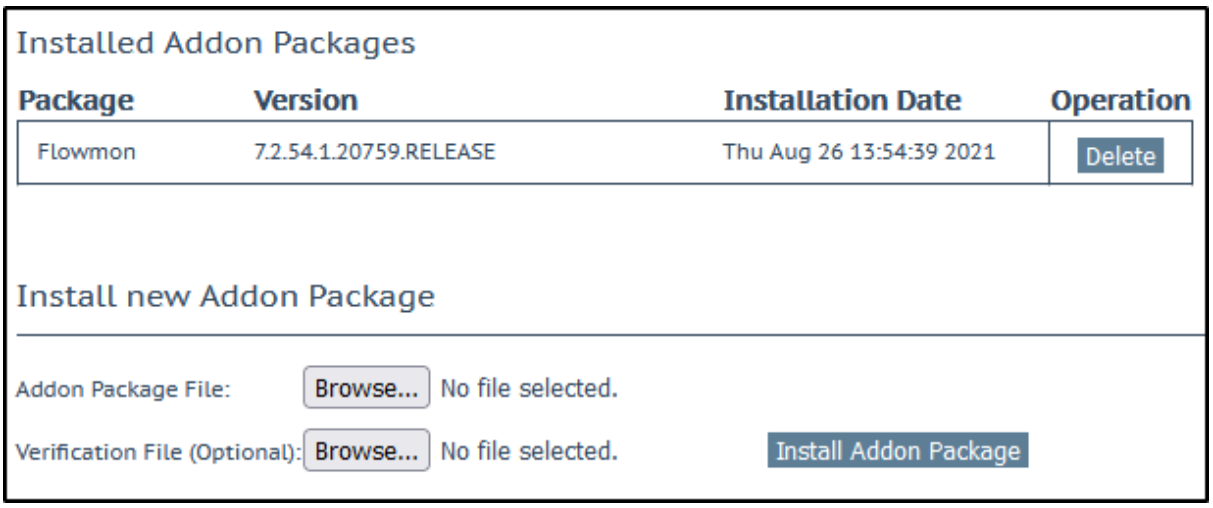
In previous releases, the updated WAF remote logging facility (**Web Application Firewall > Export Logs**) was not negotiating TLS versions above TLS 1.0. In LMOS 7.2.55, WAF has been modified to use the **Certificates & Security > Remote Access > Outbound Connection Cipher Set** setting for handshake negotiation.

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 7.2.55.0, 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 7.2.55.0 you can get the latest version of the add-on as follows:
  1. Go to the LoadMaster Add-on Packages page.
  2. Click 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 **7.2.55.0** 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:



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 7.2.55.0.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.

LoadMaster Dashboard Installer for Collector (Version 2)

A new version of the LoadMaster dashboard creation script for Flowmon Collector (supplied originally with LMOS 7.2.53.0) is available from the Other Downloads section of the support website. Key improvements in this version:

- An additional LMOS API script is provided to automate creation of the configuration file required to run the dashboard script. Like the dashboard script itself, this is a bash shell script that can be run from the Collector's SSH login shell.
- The dashboards created reflect LoadMaster settings (such as Alternate IP Address, Transparency, and Subnet Originating Requests) that affect the IP addresses LoadMaster uses to communicate with Real Servers and clients. Prompts are issues for any information that cannot be clearly identified using the API.
- SubVS traffic is now visualized on separate per-SubVS dashboards.

For complete instructions on using the scripts, see the documentation included in the download archive.

GEO: Capacity, Performance, and UI Enhancements

GEO capacity and performance have been improved in this release:

- In previous releases, the number of Fully Qualified Domain Names (FQDNs) that can be defined is limited to 256 total FQDNs. With this release, significant improvements to processing and performance have resulted in the removal of this limitation. The practical limit to the number of FQDNs supported will be determined by available system resources -- including the amount of load balanced traffic being handled by LoadMaster. As a rule of thumb, an FQDN with 64 IP addresses consumes about 2MB of memory.
- The global limit of 1024 IP addresses and records has also been removed. [Note: the limit of 64 IP addresses per FQDN remains.]
- Modifications to the FQDN UI support the above limitation changes and the UI should be generally more responsive than in previous releases.

4

Change Notices

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

Related Links

For details, see the following topics:

- SSL Renegotiation Disabled By Default
- Ciphers Use for Re-encryption
- Increased Size Limitation for SSO Custom Form Images
- RPS Limiting UI Removed for Non-Offloaded HTTPS Port 443 VSs

SSL Renegotiation Disabled By Default

Starting with LMOS 7.2.55, the **System Configuration > Miscellaneous Options > L7 Configuration > SSL Renegotiation** setting will be *disabled* by default, as a recommended security best practice. There are many published vulnerabilities with renegotiation and TLS 1.3 removes support for it completely. ***Note that this change applies to both new deployments and upgrades.***

Ciphers Use for Re-encryption

In previous releases, the ciphers used for re-encryption connections to Real Servers was not configurable.

All re-encryption connections now use the same set of ciphers used by other outbound connections, as specified by the **Certificates & Security >Remote Access > Outbound Connection Cipher Set** setting.

Increased Size Limitation for SSO Custom Form Images

The size limitation for images provided in custom image sets for Forms Based single sign on has been increased from 256 KB to 1 MB.

RPS Limiting UI Removed for Non-Offloaded HTTPS Port 443 VSs

The QoS/Limiting option for rate limiting by **HTTP Requests per Second (RPS)** will no longer appear in the UI for HTTPS Virtual Services on port 443 with **SSL Acceleration** *disabled*. **SSL Acceleration** must be enabled or this option will not appear -- the SSL connection must be terminated on LoadMaster for this option to work.

5

Security Updates

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

Related Links

For details, see the following topics:

- Update OpenSSL to Version 1.1.1k
- Strict Transport Security Header Settings
- Single Sign On: SameSite and Secure Options
- Console Support for WUI Cipher Reset
- Certificate Chain of Trust for UI Authentication
- Console CLI Security Update
- WUI Template Security Update

Update OpenSSL to Version 1.1.1k

The version of OpenSSL on LoadMaster has been updated from 1.1.1 (no letter) to 1.1.1k, to address various issues in the previously supported release.

Strict Transport Security Header Settings

HTTP Strict Transport Security (HSTS) allows a server (in this case LMOS) to set a header in client responses that instructs the client to force all subsequent connections to use HTTPS and to disregard any attempt to load any resource in that domain (and possibly its subdomains) over HTTP.

The **Strict-Transport-Security** header has various associated settings, none of which were exposed in the UI in previous releases. With this release, all settings are available through both the API and the UI. In the UI, they are exposed as follows:

- The default maximum age of all **Strict-Transport-Security** headers set by LoadMaster is 31536000 seconds (365 days/1 year). This global value can be modified on the **System Configuration > Miscellaneous Options > L7 Configuration** page by setting **L7 Security Header Age** to the desired number of seconds. Two years (63072000 seconds) is a commonly used value; the largest value that can be set is three years (94608000 seconds).
- The content of the **Strict-Transport-Security** header can be customized for each Virtual Service in the **SSL Properties** section of the VS configuration:
  - **Don't add the Strict Transport Security Header**: This is the default value.
  - **Add the Strict Transport Security Header -- no subdomains**: Adds the header only to client responses in the domain, not for any subdomains.
  - **Add the Strict Transport Security Header -- include subdomains**: Adds the header to client responses in the domain and all subdomains.
  - **Add the Strict Transport Security Header -- no subdomains + preload**: Adds the header only to client responses in the domain, not for any subdomains; allow the use of HSTS preloading, if supported by the client browser.
  - **Add the Strict Transport Security Header -- include subdomains + preload**: Adds the header to client responses in the domain and all subdomains; allow the use of HSTS preloading, if supported by the client browser.

See the following links for more information and guidelines on setting the HSTS header; also see this explanation of HSTS preloading.

Single Sign On: SameSite and Secure Options

Single Sign On data connections in previous release didn't include either a "SameSite" or "Secure" parameter in the Set-Cookie header. With this release, the "Secure" parameter is now *always* sent and, by default, the "SameSite" parameter is not added. These options can be set globally or per-Virtual Service:

- The global setting on the **System Configuration > Miscellaneous Options > L7 Configuration** page can be set to the following values:
  - **SameSite Option Not Added** (the default value, compatible with previous releases)
  - **None**
  - **Lax**
  - **Strict**
- The Virtual Service setting appears under **ESP Options** *when ESP is enabled and* ***Client Authentication Mode*** *is set to* ***Forms Based***. The default value at this level is the **System Default** setting, which means

it's the same as the global setting. The other values shown above can also be set at the VS level.

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).

Certificate Chain of Trust for UI Authentication

The ability to specify the intermediate and Certificate Authority (CA) certificates to be used to validate a client certificate presented for login to the UI has been added to the API and to the **Certificates & Security > WUI Access Options** UI page. Controls have been added to the top of the page under **Admin WUI Options** that list all the intermediate and CA certificates currently installed on LoadMaster and allow you to select the certificate(s) that will be used to validate client certificates presented for login. Any client certificates presented whose chain of trust cannot be validated using the selected CA and Intermediate certificates will be denied access. The default is to check against all existing certificates.

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.

6

Issues Resolved

PD-18853	**Logging - ESP CEF Format Logs**: Fixed various issues that could cause incorrect information to be displayed in the ESP Common Event Format (CEF) format logs.
PD-18852	**Console Security**: Addressed security issues in the console interface that could allow an authenticated user to gain access to a privileged shell.
PD-18831	**Let's Encrypt**: Fixed errors that caused domain names to be compared in a case-sensitive manner, instead of case-insensitive.
PD-18784	**Logging - ESP Performance**: Addressed issues with date calculations that could cause ESP logging to consume significant CPU resources.
PD-18737	**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-18727	**Access Control Lists (ACLs)**: In previous releases, an ACL entry that denies access to a Virtual Service would be *ignored* (and access allowed) under these conditions: • the VS uses port 443 • the VS is assigned an IP that is located on a network interface on which the User Interface (UI) is *not* running This issue has been fixed.
PD-18597	**Statistics for Client Limiting**: Fixed an issue that resulted in no limiting statistics being displayed after activating "generate limiter statistics".

PD-18594	**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-18525	**WAF**: Fixed an issue where enabling WAF on a Virtual Service did not enable statistics to be displayed.
PD-18479	**WAF**: Fixed a bug that resulted in the counters for Top 10 Countries being reset when WAF is enabled/ disabled and stop displaying data.
PD-18478	**WAF**: Fixed a bug that caused response rules to not be processed properly, resulting in WAF not blocking attacks that should have been blocked.
PD-18469	**Kubernetes Ingress Controller**: Moved internal logs that occur under some circumstances to the debug log.
PD-18466	**WAF**: Fixed issues that could cause a segmentation fault or reboot when the WAF configuration is modified while there is traffic passing through the WAF engine.
PD-18454	**ESP Post-Pass Authentication**: Fixed a bug that broke the "Post-Pass" authentication method (and hence broke preauthentication for Citrix Workspace App deployments).
PD-18448	**Health Checking**: Fixed a bug that broke the Show Headers button for the HTTP Protocol and HTTPS Protocol Real Server Check Methods.
PD-18440	**WAF**: Addressed an issue with connection timeouts that caused the log message "Hit connection limit 64000" to appear and WAF processing to stop when a remote real server fails.
PD-18437	**API V2 (JSON)**: Fixed an issue with the *addvs* command that caused a segmentation fault when an invalid configuration is supplied.
PD-18423	**API V2 (JSON)**: Fixed issues with several commands where the JSON output returned was either incorrect or empty.
PD-18295	**WAF**: Modified the permitted characters for custom WAF rule and data files to also include period and dash characters. The full set of supported characters includes: all alphanumeric characters, period (.), dash (-), and underscore (_).
PD-18292	**SNMP**: Fixed an issue that could cause the SNMP daemon to exit when many real servers are configured.
PD-18268	**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-18244	**Virtual Service UI**: Fixed issues associated with missing UI controls after converting a VS from Generic to HTTP-HTTP/2-HTTPS.
PD-18202	**LDAP UI Access**: Fixed an issue that could allow an invalid user to get UI access.
PD-18144	**GEO Clustering**: Fixed an issue that caused GEO cluster checks to fail with the log message "logger: error receiving the file from the remote LM".
PD-18140	**Logging - ESP**: Added ESP user logs when flushing the SSO cache.

PD-18137	**WAF**: Fixed a bug in Custom Rules selection that required selecting 'drupal' to enable any custom rules.
PD-18098	**WAF PowerShell API**: Added the *AlertThreshold* parameter to the *addvs* command.
PD-18043	**Real Servers**: Fixed an issue where LoadMaster failed to pass data to a Real Server with an Elliptical Curve (EC) certificate.
PD-18041	**SubVS Multiple Connect**: In previous releases, when Enable Multiple Connect is turned on for a SubVS, some connections will close if the server response body was empty. This issue has been fixed.
PD-18028	**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-18021	**Content Rule UI**: Display is incorrect when the 'Ignore case' option is enabled.
PD-17973	**Single Sign On - LDAP**: Fixed issues associated with LDAP SSO no longer working after an upgrade to LMOS 7.2.53. The issues appeared in conjunction with log messages like the following:ssomgr: ... Couldn't bind: [LDAP-AD] [*ip-addresses-omitted*]: 32, No such objectssomgr: do_sso_ldap_check: Could not get ldap_result for (*credentials-omitted*): 32 [No such object]
PD-17947	**IPv6 and Packet Filtering**: Fixed an issue that prevented IPv6 traffic from a Real Server (acting as a client) was not forwarded by the LoadMaster when packet filtering was enabled.
PD-17934	**QoS / Client Limiting**: Fixed an issue that could cause client limiting to thrash between limiting and not limiting a client.
PD-17931	**Content Response Rules**: Fixed an issue that caused performance issues when attempting to apply a response rule to an empty file.
PD-17876	**QoS/Limiting**: Fixed an issue that could cause a kernel panic when limiting UDP traffic.
PD-17867	**Historical Graphs UI**: Addressed an issue that caused some graphs to disappear from the page following upgrade to v7.2.53.
PD-17719	**RADIUS Health Checks**: Fixed an issue where RADIUS health checks with very long re-authentication times stop working after upgrade to LMOS 7.2.52.
PD-17601	**Syslog CEF Logging**: Fixed issues where Common Event Format logging is enabled and some user logs are improperly merged because of spurious characters (%5c) in the login string.
PD-17451	**API V2 (JSON)**: Fixed an issue where the *listfqdns* API V2 was returning and invalid JSON response with duplicate keys. The parameters are now properly wrapped inside an array.
PD-16140	**GEO**: Fixed an issue that caused TXT records to be blank after 1024 IP addresses are added to an FQDN.
PD-15585	**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.

7

New Known Issues

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.
PD-19175	**ESP User Logs**: It is possible that the domain name reported in a login message and an associated kill session message do not match.

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.

8

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-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-15633	**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.
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-152	**ESP Verify Bearer Header**: LoadMaster does not return an error when an encrypted token is received and

94	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 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	**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.