

LoadMaster 7.2.48.2 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: Supported Models for Upgrade 6

Chapter 3: Upgrade Path 8

Chapter 4: New Features 9

IPv6 Certification 9

DHCPv6 Support 10

Azure Support for 10 Gb Interfaces 10

IRQ Pinning 10

Minimum Password Length 10

Console Logging Enhancements 11

Securing Outbound Connections 11

OCSP Stapling for Outbound Connections 11

Elliptic Curve Cipher Sets 11

Elliptic Curve Self-Signed Certificates 12

Elliptic Curve Certificate Signing Requests 13

Secure Factory Reset 13

High Availability Broadcast Support 13

Chapter 5: Change Notices 14

Signature Verification of Updates and Add-Ons Required By Default 14

Log Format Enhancements 15
Specifying the Protocol for Remote Logging 15
Custom HTML Files for Redirection Handling Added to Backup 15

Chapter 6: Security Updates 16
Updated NIST FIPS Cryptographic Module Certification 16
Assigning Intermediate Certificates to Virtual Services 17
Syslog and LDAPS Server Certificate Validity Checking 17
Enhanced Random Number Generator Seeding 17

Chapter 7: Issues Resolved 19

Chapter 8: Existing Known Issues 22

1

Introduction

LMOS Version 7.2.48.2 is a feature and bug-fix release made available in November 2020. Please read the sections below before installing or upgrading.

2

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.

3

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.

4

New Features

The following new features have been added to this release of LMOS.

Related Links

- IPv6 Certification
- DHCPv6 Support
- Azure Support for 10 Gb Interfaces
- IRQ Pinning
- Minimum Password Length
- Console Logging Enhancements
- Securing Outbound Connections
- OCSP Stapling for Outbound Connections
- Elliptic Curve Cipher Sets
- Elliptic Curve Self-Signed Certificates
- Elliptic Curve Certificate Signing Requests
- Secure Factory Reset
- High Availability Broadcast Support

IPv6 Certification

LMOS 7.2.48.2 was submitted to the University of New Hampshire InterOperability Testing Laboratory and

successfully passed testing for IPv6 and DHCPv6 certification under the USGv6 program, a U.S. Government program for certifying that a tested device can interoperate according to relevant standards with other devices in an IPv6 network. Final certification was obtained in September 2020.

All versions of LMOS above 7.2.48.2 are also similarly certified, since they use the same certified IPv6 stack. For a full test report, please see the UNH Testing Registry for a full test report.

See the LoadMaster IPv6 Configuration Guide for detailed IPv6 configuration instructions.

DHCPv6 Support

Support for DHCPv6 (Dynamic Host Configuration Protocol for IPv6) has been added for initial LoadMaster deployment and can optionally be enabled afterwards, if required.

On initial deployment, both DHCPv4 and DHCPv6 are enabled and attempt to obtain an IP address. After an IP address is obtained (either via DHCP or by assigning the fallback IPv4 address of 192.168.1.101), DHCP is disabled and will remain disabled until manually reactivated via the API or using the **Enable DHCPv6 Client** check box on the **System Configuration > Logging Options > System Log Files > Debug Options** page of the UI.

When this option is enabled, the DHCPv6 client runs on the primary interface to obtain an IPv6 address and will remain running across subsequent reboots until this option is disabled. It is recommended that DHCPv6 be disabled after an IPv6 address is obtained, unless you are running the system within an IPv6 network where running DHCPv6 during normal system operation is required.

Azure Support for 10 Gb Interfaces

Support for 10 Gb interfaces on the Azure cloud platform complements the 10 Gb interface capabilities introduced in previous releases of LMOS for the AWS platform. For details on how to choose 10 Gb capable machine sizes when deploying LoadMaster on Azure, see the LoadMaster Deployment Guide for Azure.

IRQ Pinning

For virtual LoadMaster deployments, LoadMaster has been enhanced to provide IRQ Pinning as an optional performance enhancement, via controls in the UI and API. When enabled, IRQ pinning can help LoadMaster distribute the system load to more efficiently use resources, which can help improve performance under specific load profiles. IRQ pinning is disabled by default.

Minimum Password Length

A new control on the **System Configuration > System Administration > User Management** page allows you to set a global **Minimum Password Size** for local LoadMaster user logins. The default length is 8 characters and can be set to any value up to 16.

Console Logging Enhancements

The system console interface has been enhanced to log all actions taken by a user logged into the console to improve troubleshooting and administrative accountability.

Securing Outbound Connections

In previous releases, not all outbound connections originated by LoadMaster were encrypted. A new control on the **Remote Access** UI page, **Outbound Connection Cipher Set**, allows you to select a pre-defined cipher set to be used for all outbound connections, including:

- Remote logging (syslog)
- Email notifications
- LDAP authentication
- OCSP certificate validation

The default setting is **None**, for compatibility with previous releases.

OCSP Stapling for Outbound Connections

LoadMaster has been modified to apply Online Certificate Status Protocol (OCSP) stapling (if enabled) to verify certificates for all external connections originated by LoadMaster, except for re-encrypted connections to real servers.

Elliptic Curve Cipher Sets

Two new cipher sets have been added, as shown below, specifically for configurations that require elliptic curve ciphers:

ECDSA_Default	ECDSA_BestPractices
ECDHE-ECDSA-AES256-GCM-SHA384	ECDHE-ECDSA-AES256-GCM-SHA384
DHE-DSS-AES256-GCM-SHA384	DHE-DSS-AES256-GCM-SHA384
ECDHE-ECDSA-CHACHA20-POLY1305	ECDHE-ECDSA-AES256-SHA384
ECDHE-ECDSA-AES256-CCM8	ECDHE-ECDSA-AES256-SHA
ECDHE-ECDSA-AES256-CCM	DHE-DSS-AES256-SHA
ECDHE-ECDSA-ARIA256-GCM-SHA384	ECDHE-ECDSA-AES128-GCM-SHA256
DHE-DSS-ARIA256-GCM-SHA384	DHE-DSS-AES128-GCM-SHA256

ECDSA_Default	ECDSA_BestPractices
ECDHE-ECDSA-AES256-SHA384	ECDHE-ECDSA-AES128-SHA256
DHE-DSS-AES256-SHA256	ECDHE-ECDSA-AES128-SHA
ECDHE-ECDSA-CAMELLIA256-SHA384	DHE-DSS-AES128-SHA256
DHE-DSS-CAMELLIA256-SHA256	
ECDHE-ECDSA-AES256-SHA	
DHE-DSS-AES256-SHA	
DHE-DSS-CAMELLIA256-SHA	
ECDHE-ECDSA-AES128-GCM-SHA256	
DHE-DSS-AES128-GCM-SHA256	
ECDHE-ECDSA-AES128-CCM8	
ECDHE-ECDSA-AES128-CCM	
ECDHE-ECDSA-ARIA128-GCM-SHA256	
DHE-DSS-ARIA128-GCM-SHA256	
ECDHE-ECDSA-AES128-SHA256	
DHE-DSS-AES128-SHA256	
ECDHE-ECDSA-CAMELLIA128-SHA256	
DHE-DSS-CAMELLIA128-SHA256	
ECDHE-ECDSA-AES128-SHA	
ECDHE-ECDSA-RC4-SHA	
DHE-DSS-AES128-SHA	
DHE-DSS-CAMELLIA128-SHA	

Elliptic Curve Self-Signed Certificates

A new option on the **Certificates & Security > Remote Access** page of the UI allows you to select from among these options for self-signed certificates for Administrative Access:

- RSA self-signed certs: (Default) This is the only setting on legacy releases of LMOS. The certificate used will be an RSA certificate signed with the Kemp RSA root certificate.
- EC certs with a RSA signature: The certificate used will be an RSA certificate signed with the Kemp EC (elliptic curve) root certificate.
- EC certs with an EC signature: The certificate used will be an EC certificate signed with the Kemp EC

(elliptic curve) root certificate.

Elliptic Curve Certificate Signing Requests

A Certificate Signing Request for an SSL Certificate can be created using the controls on the **Certificates & Security > Generate CSR** UI page. By default, CSRs generated by LoadMaster request an RSA-encrypted key. If you enable the **Generate Elliptic Curve Request** option on this page, LoadMaster instead requests an ECC (elliptic curve) key. Smaller ECC key sizes generally provide the same cryptographic strength as much larger RSA key sizes; and, so ECC keys are becoming increasingly common because of both the reduced storage footprint as well as processing resources required.

Secure Factory Reset

The factory reset option has been enhanced to securely reset the system configuration by not only deleting the files, but also erasing the content of the files from the disk so that any examination of the disk contents will not reveal any deleted data.

High Availability Broadcast Support

In past releases, LoadMaster High Availability (HA) status information was communicated between HA partners over a multicast IP address (224.0.0.*x*); there was no other option. With this release, a new HA parameter (**Use Broadcast IP address**) can be optionally set to use the broadcast IP address 255.255.255.255 instead of a multicast address. This allows HA configurations to be established on networks where the use of multicast IP addressing is specifically disabled.

5

Change Notices

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

Related Links

- Signature Verification of Updates and Add-Ons Required By Default
- Log Format Enhancements
- Specifying the Protocol for Remote Logging
- Custom HTML Files for Redirection Handling Added to Backup

Signature Verification of Updates and Add-Ons Required By Default

Starting with this release, by default, signature verification files must be supplied with upgrade images and add-on packages on installation on the **System Configuration > System Administration > Update Software** page. Installation will not be permitted unless the usual update integrity checks *and* the additional signature verification check succeed.

This behavior can be controlled by changing the setting of the **Update Verification Options** setting on the **System Configuration > Miscellaneous Options > WUI Settings** page. There are three settings available:

- **Required**: (Default) The signature verification file settings are visible and providing the signature file is mandatory.
- **Optional:** The signature verification file settings are visible, but providing the signature file is optional.

- **No verification file - deprecated**: (Not Recommended) The verification file settings are not visible and providing the signature file is not possible in the UI. This is the legacy setting used in older LMOS releases and is included for backwards compatibility only.

Note that the *update integrity checks* mentioned above cannot be disabled and must always succeed in order for an installation to proceed.

Log Format Enhancements

The system log and ESP extended log messages have been enhanced to be compliant with Section 6 of RFC 5424. This will aid local troubleshooting as well as external analysis of LoadMaster log messages by 3rd-party log collector and analysis tools.

Specifying the Protocol for Remote Logging

In previous releases, the remote logging functionality assumed the protocol to use based on the port specified: UDP for port 514 and TCP for all other ports. A new **Remote Syslog Protocol** control has been added to the **System Configuration > System Administration > Logging Options > Remote Syslog** page of the UI to either UDP, TCP, or TLS, independently of the port number.

Custom HTML Files for Redirection Handling Added to Backup

The backup and restore subsytem has been enhanced to include all custom HTML files associated with redirection handling for a Virtual Service (VS) included in a backup archive, and to restore these files from the archive onto the target system along with the rest of the VS configuration.

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

- Updated NIST FIPS Cryptographic Module Certification
- Assigning Intermediate Certificates to Virtual Services
- Syslog and LDAPS Server Certificate Validity Checking
- Enhanced Random Number Generator Seeding

Updated NIST FIPS Cryptographic Module Certification

Kemp has updated its NIST FIPS Cryptographic Module Certification, the new certificate can be viewed on the NIST website here.

Assigning Intermediate Certificates to Virtual Services

Starting with this release, specific intermediate certificates can be assigned to Virtual Services, using controls within the **SSL Options** accordion in the UI. The default behavior, and the behavior in previous releases, is that all installed intermediate certificates will apply to a VS; this means that any client certificate presented that uses an intermediate certificate found on LoadMaster will be accepted and access to the VS will be granted. Once one or more intermediate certificates is selected in a VS configuration, only client certificates that have one of those specific intermediate certificates in their certificate chain will be granted access to the VS.

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 Random Number Generator Seeding

In previous releases, seeding the system random number generator was performed on all platforms using entropy sources that were available directly to the kernel after boot, providing an acceptably high level of entropy. Best practices in the industry (e.g., Common Criteria) have evolved to generally recommend that, when available, systems running on Intel architectures take advantage of Intel's **Digital Random Number Generator** (DRNG) software to provide additional entropy sources from the processor at boot time.

LoadMaster has been enhanced to attempt to use the Intel DRNG architecture's RDSEED and RDRAND processor instructions to provide additional entropy for seeding the random number generator. This behavior is disabled by default; to enable:

1. In the UI, navigate to **Certificates & Security > Remote Access.**
2. Set the **Self-Signed Certificate Handling** option to **EC certs with an EC signature.**
3. Reboot LoadMaster.

On the next boot, LoadMaster will attempt to use RDSEED as an entropy source and, if that fails, RDRAND. If successful, the message **sslproxy: Initial Random Vector** appears in the system log.

All current LoadMaster hardware supports either RDSEED or RDRAND, as do many legacy hardware platforms. Whether or not this option can be used for a Virtual, Cloud, or Bare Metal LoadMaster deployment depends entirely on the processor of the hardware platform on which the hypervisor is running.

If the processor *does not* support RDSEED/RDRAND, then LoadMaster becomes unavailable due to the lack of an "approved" entropy source. The following occurs:

- The UI displays only this message (no functionality):

  ```
  Could not start CC mode - system disabled.
  ```

- A CRITICAL log message is created in the messages file:

  ```
  Cannot initialize RNG, CC mode disabled.
  ```

- An authlog messages is also created.

  ```
  Failed to start RNG, CC mode not started.
  ```

To get out of this mode, you have to log into the system console, navigate to the Local Administration > Web Address screen, and select **Confirm switch out of CC mode**. Once the system restarts, you will be able to access the system as usual, but it will not operating in Common Criteria mode -- the kernel will generate entropy after boot as in previous releases. This is evidenced by the following **authlog** message:

```
User disabled CC mode.
```

7

Issues Resolved

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

PD-15228	**HTTPS Ciphers**: Previously, assigning a cipher set that contains all available ciphers to an HTTPS Virtual Service (VS) will causes the VS to become unresponsive. This bug has been fixed so that it's now possible to assign a cipher set that contains all available ciphers to a VS
PD-15206	**ESP / SSO**: When using ESP on a Virtual Service and **Use for Session Timeout** is enabled, a user is not completely logged out when an OWA session is terminated. This issue has been fixed.
PD-15202	**RESTful API**: Changing the remote syslog port using the API doesn't result in the new port being enabled. This bug has been fixed.
PD-15179	**IPv6**: IPv6 routing changes for standards conformance in the previous release caused IPv6 static routes to no longer be honored. This issue has been addressed by introducing a new option on the Debug Options page, **Enable Layer 4 IPv6 Forwarding**. This option is enabled by default to support pre-7.2.50 LoadMaster behavior and should be disabled if IPv6-standard-conformant behavior is required.
PD-15185	**Logging**: Modified the logging of SSL messages so that handshake failures and other errors (e.g., Unsupported Protocol, No Shared Cipher, Wrong Version Number) currently seen at the **Fatal errors only** setting are only reported when **All Errors** is selected.
PD-15184	**RESTful API**: Fixed an issue that intermittently caused the *ssodomain/queryall* API to return an error.
PD-15133	**ESP SSO Logoff**: In LMOS 7.2.50, an issue was introduced where Single Sign On sessions on LoadMaster were not being properly removed upon logoff, causing subsequent login attempts to fail. This issue has been fixed.

PD-150 54	**Manage Services UI**: Fixed an issue where the indicator for the SubVS with the highest numerical weight (a green star) did not move to the appropriate SubVS if another SubVS's weight changed so that it was higher than the SubVS with the indicator.
PD-150 21	**VMware Deployment**: VMware images have been modified so that the CLI will no longer return the message "init ID S0 respawning too fast: disabled for 5 minutes".
PD-149 85	**ESP Single Sign On**: Fixed an issue that caused a refresh of a login page to display an access denied page, even if the allowed virtual host and virtual directories were set to wildcards.
PD-148 57	**Single Sign On**: Fixed an issue that caused a segmentation fault during an LDAP domain health check when the second bind attempt succeeds.
PD-148 53	**UI on Nutanix Platform**: In previous releases, under the **Real Time Statistics**, the speed shown for interfaces on the Nutanix cloud platform was displayed as "-1". Now, the speed displayed will be dependent on the amount of load placed on the interfaces
PD-148 25	**Single Sign On Logging**: Fixed an issue that caused Single Sign On related log messages to be duplicated in more than one log file.
PD-147 54	**Server Side Re-encryption**: Fixed a bug that caused server-side re-encryption to close connections with a TCP FIN/ACK sequence instead of the required TCP RST (reset) packet, when the **Enable Reset on Close** option is enabled.
PD-147 48	**Virtual Service SNAT**: In previous releases, if you disable a Real Server in a VS that is using SNAT and then re-enabled the Real Server, SNAT is silently disabled for that Virtual Service. This bug has been fixed.
PD-147 46	**RADIUS Two-Factor Authentication**: Fixed an issue that caused a segmentation fault when a challenge response from an OTP (one-time password) server does not contain PW_STATE AVP.
PD-146 44, PD-145 50	**HTTP/2 & Compression**: In previous releases, if errors occur in HTTP/2 processing and compression is enabled, the system may reboot because the cache has not been properly released. This issue has been fixed.
PD-144 34	**PowerShell API Certificate Limit**: The PowerShell API is limited to about 1K characters for the list of certificate names, while the limit in the UI is a little under 8K. This issue in the API has been addressed.
PD-144 26	**Content Rules**: Content rule names can now use a numeric character as the first character in the name.
PD-144 15	**Stability and Reliability**: Fixed an issue seen in 7.2.48.1 and 7.2.49.1 that caused a kernel panic when running a mix of UDP, HTTP, HTTPS, SMTP, and RDP services.
PD-143 53	**UI**: Statistics displays have been modified to use the correct abbreviations for bit and byte statistics (e.g., Mb for Megabits and MB for Megabytes).
PD-143 49	**Virtual Service Templates**: In previous releases, if a VS was exported as a template and had the **Strict Transport Security Header** field set to **Add the Strict Transport Security Header - no subdomains** or **Add the Strict Transport Security Header - include subdomains**, then the template would fail with a syntax error on import to any other LoadMaster. This issue has been fixed.
PD-143 45, PD-140 09	**Single Sign On**: Fixed an issue where extending the SSO Session Timeout and the Idle Timeout does not result in the extension of the expiry of the LoadMaster session cookie.As part of this fix, the upper limit for these timeouts was extended to 7 days (or 604800 seconds in the API).

PD-14374	**HyperV Platform Boot Error**: In previous releases, a *fill_rand* error was seen on the console during boot of a VLM on HyperV 2019. This issue has been fixed.
PD-14346, PD-14039	**LDAP Remote User Groups**: Starting with LMOS 7.2.48.0, a user could under certain circumstances be granted the permissions specified for a group to which they didn't belong. This issue has been fixed.
PD-14258	**SSO**: An issue was introduced in LMOS 7.2.48.1 that caused the login form to be redisplayed even though correct credentials had been given, under specific circumstances. This issue has been fixed.
PD-14247	**UI Login**: Fixed issues that caused username/password prompts to be displayed for a local user configured for certificate-based login only.
PD-14100, PD-14050	**Exchange 2016 Outlook Web Access and Authentication Proxy Virtual Services**: Starting with LMOS 7.2.48, clients can be logged out immediately after supplying correct credentials. This issue has been fixed.

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.