Progress®
Kemp® LoadMaster®

LoadMaster 7.2.60.0 Release Notes

Generated on: 11 March 2025

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: New Features 9

Chapter 4: Change Notices 11

Chapter 5: Security Updates - Removed Weak Ciphers from Best Practices Cipher Set. 13

Chapter 6: Issues Resolved. 14

Chapter 7: Existing Known Issues 18

1

Introduction

LMOS Version 7.2.60.0 is a feature and bug fix update of the General Availability (GA) branch made available on 17 July 2024. Please read these release notes before upgrading to this version.

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 this release, the **BestPractices** cipher set was updated to remove two ciphers that are considered weak. This change was made to improve security and conform to the latest industry best practices. This change is effective immediately after upgrading to this release. For further details, refer to the following section: Security Updates - Removed Weak Ciphers from Best Practices Cipher Set (later in this document).

Note: If you depend on any of the cipher sets being removed from the **BestPractices** set, then before you upgrade you should 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.

Contents

- 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 (for example, Service Provider License Agreement (SPLA) or Metered Enterprise License Agreement (MELA)) or platform (for example, hardware, local cloud, or 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		

Supported Virtual Models	Supported Hardware Models	Supported Bare Metal Models	Unsupported Hardware & Virtual Models
	LM-8000		
	LM-8020		
	LM-8020M		
	LM-X3-NG		
	LM-X15-NG		
	LM-X25MT-NG		
	LM-XHC55-NG		
	LM-XHC75-NG		
	LM-XHC100-NG		

If your model number is not listed above, refer to 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 one of the following documents:

- Updating the LoadMaster Software Technical Note (Long Term Support Feature (LTSF) version)
- Updating the LoadMaster Software Technical Note (General Availability (GA) version)

Contents

- 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 must 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 follow the upgrade path detailed in the Updating the LoadMaster Software Technical Note article.
- Appliances 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.

Contents

- Code Signing Certificate Update

Code Signing Certificate Update

On 27 May 2022, the certificate used to sign LoadMaster release artifacts for LoadMaster LMOS version 7.2.56.x and prior releases expired. For most customers, this will not impact normal operations, as explained in this article LoadMaster Code Signing Certificate Expires 27 May 2022.

All releases that occur after the above date (for example, LMOS 7.2.57.0) will be digitally signed using a newly obtained code signing certificate.

3

New Features

Refer to the following sections for details about the new features released in version 7.2.60.0.

ACME Wildcard Certificates and DNS Challenge

In previous releases, the ACME certificate feature only supported the HTTP-01 challenge when obtaining a new certificate. With this release, the ACME DNS-01 challenge is now supported. This allows customers to obtain wildcard certificates from supported ACME providers. For further details, refer to the **Let's Encrypt** and **DigiCert** Feature Descriptions on the Certificates documentation page.

Per-VS Parameters for Resource Based Adaptive Scheduling

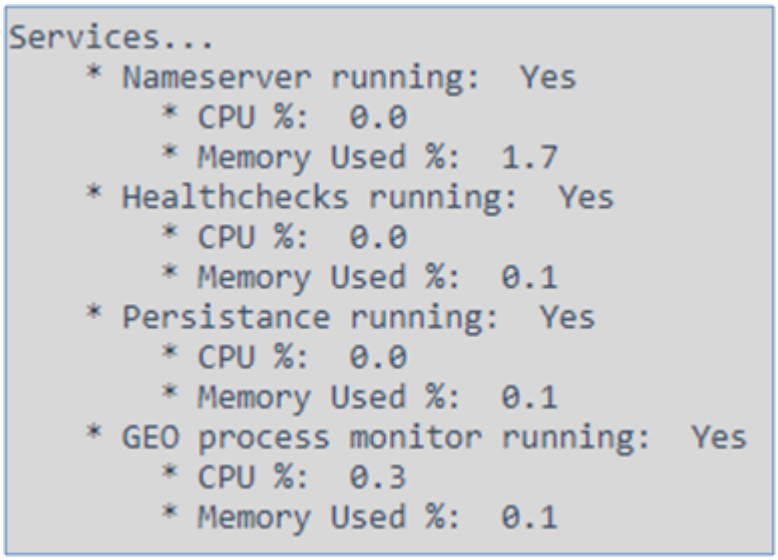
In previous releases, the operational parameters for resource based adaptive scheduling could only be set globally – with the same parameters applying across all Virtual Services that have adaptive scheduling enabled.

With this release, the global settings can now be overridden by applying different settings on the Virtual Service. For further details, refer to the Standard Options section of the Web User Interface (WUI) Configuration Guide and search the page for **Resource Based (Adaptive)**.

GEO Process Watchdog

A GEO process watchdog now continuously monitors the health of critical GEO processes. The monitor is enabled by default (as you can see on the **Global Balancing > GEO System Info/Debug** page; the

watchdog process is the last one listed):



If the watchdog detects that one of the other services is not running, it attempts to restart it. This is reflected in the system log; for example:

```
logger: named is down
```

```
logger: A GEO process has failed, restarting GEO, attempt 1
```

Note that there is a **Disable Process Monitor** button on the page to disable the process monitor, but this should only be used when debugging GEO issues. The enabled/disabled state of the process monitor is synchronized between a High Availability pair, but is *not* synchronized between GEO partners.

4

Change Notices

Refer to the following sections for details on the change notices relating to the 7.2.60.0 release.

Upgrade BIND to version 9.16.25

The version of BIND used on the system has been updated from 9.16.24 to version 9.16.25. Refer to the BIND release notes for details about the new features and other notes on this release. The major updates in this release are memory consumption enhancements aimed at restoring performance losses seen in 9.16.24 and earlier 9.16 releases. For more information on this topic, refer to https://kb.isc.org/docs/bind-memory-consumption-explained.

Default for Local Certificate Validation Modified

In previous releases, the default setting of the **Certificates & Security > Remote Access > Allow Client Certificate Login Without Locally Installed User Certificate** option was **enabled** to support legacy local client certificate behavior. [Note that this option only appears in the User Interface (UI) if you have **Admin Login Method** (on the same page) set to one of the client certificate options.]

The legacy behavior is that users logging into the system using a local certificate can continue to use the locally-generated client certificate even after the expiration date of the certificate.

Starting with this release:

- The default value of the above option is **disabled** for new deployments – which means that the legacy behavior is not supported by default.
- On upgrade, the setting for this option on the previous release (if supported in that release) is preserved.

If you have units enabled for local certificate login, we strongly recommend that you disable this option as soon as possible to maintain the strictest security profile for local user logins.

Local certificates can be generated (and re-generated) for each of the defined **Local Users** on the **System Configuration > System Administration > User Administration** page.

The 'httpOnly' Flag Added to Persistence Cookies

Cookie-based persistence has been enhanced by adding the httpOnly flag to all cookies generated by the system. This cookie attribute instructs web browsers to not allow scripts to access the cookie and helps prevent session ID stealing through XSS attacks.

Virtual Service API

Modified the way Virtual Service (VS) persistence is reported when set to “none” to be consistent with other parameters. In previous releases, the value was omitted when set to “none”; now it is explicitly reported as “none”.

Single Sign On support for non-standard ports

In previous releases, it was required to make some manual modifications when attempting to enable Single Sign On on a Virtual Service that did not use either port 80 or port 443. Starting with this release, no manual modifications are needed – they are made automatically by the system when SSO is enabled on the Virtual Service.

UEFI Boot Support

Support for the Unified Extensible Firmware Interface (UEFI) has been added. All NG hardware models use this interface.

5

Security Updates - Removed Weak Ciphers from Best Practices Cipher Set

The **BestPractices** cipher set has been updated to remove two weak ciphers:

- ECDHE-RSA-AES256-SHA384
- ECDHE-RSA-AES128-SHA256

The above are the names used in OpenSSL and on the system. They are also known by the following names:

- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256

These ciphers are considered weak because of their use of CBC. In recent years, a set of attacks on CBC ciphers in SSL/TLS have been reported as well as timing and padding attacks.

Note that these ciphers remain available on the system and can be configured into a custom cipher set if required.

6

Issues Resolved

LM-6219	**Virtual Services UI**: Fixed an issue that caused a Virtual Service to be marked as available (up) when it is actually unavailable (down).
LM-6172	**Partner Communication**: After setting the same shared secret on both partners, an Unauthorized Remote Machine error is observed. This issue has been fixed.
LM-6162	**Partner Communication**: Fixed an issue that could mistakenly cause a shared secret password banner to appear on the User Interface (UI) Home page on a non-shared IP address (for example, a stand-by node or non-admin node).
LM-6146	**Clustering**: Fixed an issue that caused a deleted node to reappear in the configuration after rebooting the admin node.
LM-6006	**Partner Communication**: Fixed an issue where (in Azure or AWS) GEO partnering did not work once the shared secret is set.
LM-6005	**Partner Communication**: Fixed an issue where (in Azure or AWS) High Availability (HA) mode did not work once the shared secret is set.
LM-5988	**GEO**: Fixed an issue that allowed a user logged in with administrative privileges to execute arbitrary commands on the system using a carefully crafted domain modify Application Programming Interface (API) command.
LM-5966	**SAML Authentication**: Differences in case between the URL and the "IdP Entity ID" parameter cause SAML authentication to fail. This has been fixed by modifying the comparison between the URL and ID to be case-insensitive.
LM-5939	**OIDC/OAuth Authentication**: An error in state validation can cause users to be logged in incorrectly. This

	issue has been fixed.
LM-5865	**NG Hardware**: Fixed an issue where VLANs do not work on 10Gb interfaces.
LM-5638	**LDAP Group WUI Authentication**: Fixed an issue where LDAP groups did not work with alternate UPNs.
LM-5606	**SAML Authentication**: Fixed an internal issue where SAML authentication succeeds, but the user is then redirected to an incorrect URL.
LM-5370	**Virtual Service API**: Modified the way Virtual Service persistence is reported when set to “none” to be consistent with other parameters. In previous releases, the value was omitted when set to “none”; now it is explicitly reported as “none”.
LM-5331	**Azure VLM**: Fixed issues that could cause the */var/log/waagent* folder to fill to capacity.
LM-5305	**Console**: The system console’s “Show Allowed Addresses” screen was titled “blocked” instead of “allowed”. This issue has been fixed.
LM-5229	**Network Telemetry**: The Flowmon probe process was not started for an interface without a shared IP address on a system configured in High Availability (HA) mode. This issue has been fixed.
LM-5228	**ACME Certificates**: Fixed an issue where requesting a new ACME certificate could cause configuration corruption.
LM-4907	**Kubernetes Ingress Controller (KIC)**: Fixed an issue that caused several minutes of delay in displaying the Kubernetes settings.
LM-4403	**SSO**: Fixed an issue that caused the error message “ssomgr: ERROR: ssomgr too many threads” to appear in the logs, sometimes followed by a segfault.
LM-3164	**Remote Logging**: Optimized the flow for sending syslog messages to the remote syslog device to reduce local resources consumed.
LM-3127	**WAF Custom Rules**: Added custom rules validation on upload to flag a CIDR address with a "/32" suffix as an error. The Web Application Firewall (WAF) engine requires single IP addresses to be specified *without* the “/32” suffix.
LM-3096	**WAF Custom Rule Data Files**: Fixed an issue where spurious text may be displayed in the UI when uploading a custom rule data file.
LM-3014	**PowerShell API**: Added a "Confirm" flag to the *installpatch* API to match the REST API.
LM-2802	**GEO Clustering**: Fixed an issue that causes spurious log messages to be generated when a system boots that is configured with at least one GEO Cluster.
LM-2777	**GEO RestAPI**: Fixed a regression in the *listclusters* API introduced in 7.2.55.0. In that release, the cluster IP address field name was inadvertently changed to “Addr”. With this release, it has been changed to its pre-7.2.55.0 name, "IPAddress".
LM-2767	**WAF**: Fixed an internal issue where a null character in a request URI could cause truncation of the request before it is examined by the WAF engine, possibly resulting in an incorrect analysis of the URI.
LM-2762	**SAML Authentication**: Fixed an issue that caused SAML authentication to fail when using 4K key lengths.
LM-2731	**OIDC/OAuth Authentication**: Fixed an issue where the UI rejects a valid application secret generated from a PowerShell API script.

LM-2651	**GEO RestAPI**: Fixed an error that results in information regarding a deleted Virtual Service still being displayed in the *listclusters* API output, after the Virtual Service is deleted.
LM-2627	**GEO**: Fixed an issue where locations for IPv6 addresses are not returned in a DNS response when specifying an IPv6 address for the EDNS client subnet.
LM-2566	**Persistence**: Fixed an internal issue that can cause server cookie persistence to break for some requests when 'Always Check Persist' is enabled.
LM-2474	**Log Message Priority**: Changed the severity level of 'Being too busy...' log messages to Informational (from Error) to reflect its significance.
LM-2470	**GEO**: Fixed an issue where performing a PTR query on an FQDN (rather than on an IP address in a PTR record) results in a segfault.
LM-2447	**GEO Clustering**: Fixed issues that caused GEO to misjudge the health of LoadMasters in Clustering mode. GEO Clustering also now works when deployed on a LoadMaster in Clustering mode.
LM-2446	**GEO**: Fixed a possible internal buffer overflow issue that could be triggered by character expansion.
LM-2439	**Logging**: Addressed inconsistencies between messages logged for L7 and the SSOMGR in non-debug and debug modes.
LM-2423	**ACME Certificates**: Fixed an issue where a certificate added to a Virtual Service for re-encryption does not appear in the list of Virtual Services (associated with that certificate) on the ACME certificates page.
LM-2398	**Kubernetes Ingress Controller (KIC)**: Fixed an issue where a manually removed Real Server is not re-added to the Virtual Service by the controller.
LM-2396	**PowerShell API**: On the KVM platform only, the *getall* command fails with the message: “Error connecting to device due to Invalid parameter on KVM”. This issue has been fixed.
LM-2357	**Clustering**: Starting with 7.2.58.0, some Virtual Services in the Cluster may be spuriously marked down due to the incorrect internal processing of Real Server status.
LM-2355	**PowerShell API**: The *Get-ACMEAccountInfo* command fails because the type is not specified, but there is no type parameter. This issue has been fixed.
LM-2034	**GEO**: Since 7.2.55.0, the Real Server Connection selection criteria is not distributing traffic as expected. This issue has been fixed.
LM-1924	**PowerShell API**: Starting with 7.2.58.0, the *Backup-LmConfiguration* command returned a 400 error (protocol violation / invalid header name). This issue has been fixed.
LM-1902	**Networking**: Modified the handling of the default gateway interface so that the IP address of the interface cannot be removed if the default gateway is defined on that interface.
LM-1892	**Single Sign On**: Fixed an internal issue that could cause a segfault in the SSO Manager process when SAML and Kerberos Constrained Delegation (KCD) were configured.
LM-1878	**GEO Custom Locations**: Fixed an issue where deleting a Custom Location Name could (under some circumstances) cause the GEO configuration to be corrupted.
LM-1867	**Virtual Service Redirects**: When an existing port 80 service is modified to redirect traffic to port 443, the Error Page still takes precedence when changing the Status Code from 200 to another Status Code. This issue has been fixed.

LM-1830	**GEO**: When using manual site recovery a "Failing" IP remains "Failing" even if it has come back up. This issue has been fixed.
LM-1800	**Azure VLM**: Fixed issues that could cause the */var/log/waagent* folder to fill to capacity.
LM-1743	**FIPS Mode Custom Cipher Sets**: Fixed an issue where, after changing the system into FIPS mode, custom cipher sets still contained restricted ciphers.
LM-1709	**Virtual Services**: Addressed issues that caused a Virtual Service to stop responding to requests randomly when a specific number of content rules have been created.
LM-1450	**GEO API**: Fixed an issue where "Zone Name" and "ZOA Email" are missing from the Miscellaneous GEO Parameters returned by the API.
LM-1370	**REST API**: Fixed an issue that caused the *unlockdomainusers* API to return success when the user has not been unblocked, or when a parameter is incorrect.
LM-1342	**Kubernetes Ingress Controller (KIC)**: Fixed an issue that caused the ingress controller to stop working when the default admin gateway is changed.
LM-1340	**GEO UI**: Clarified the error message received on adding an FQDN that contains more than the permitted number of characters.
LM-1325	**ACME Certificates**: Fixed an issue that could cause the certificate creation page to be only partially displayed.
LM-1323	**Automated IP Access List Data Update**: Improved the error message received when a download of the list fails.
LM-968	**Online Certificate Status Protocol (OCSP)**: Modified connection processing for OCSP servers that have keepalive enabled.
LM-137	**Kerberos Constrained Delgation (KCD)**: Fixed an issue that caused multiple logs to be written for a single login failure.
LM-123	**GEO UI**: Modified the default values for location coordinates so that they are the same across the UI.
LM-116	**Real Time Statistics**: Fixed an issue where the “Current rate - Conns/sec” under RS Totals does not match the “Current rate - Conns/sec “under Real Servers.

7

Existing Known Issues

LM-2749	**API Keys**: An API key created for a remotely managed user (for example, RADIUS) will not work unless the remote user ID is also added as a local user on the LoadMaster.
LM-1865	**WAF Audit Logs**: No output is returned when selecting a date range.

LM-1557	**Single Sign On**: A segmentation fault in the SSO management process can occur under high load resulting in users being logged out. Messages like the following will be seen in the log:
	
	`kernel ssomgr[46119]: segfault at <num> ip <num> sp <num> error 4`
	`kernel L7: verify_user: Auth request failed for id 0`

LM-1527	**GEO Cluster Checks**: GEO cluster checks against LoadMasters configured in Clustering mode do not work.
LM-1412	**API stats command**: On a unit in Clustering mode, the up/down status value returned by the stats command may be different (and incorrect) compared to the status returned by **listvs** or **vstotals**.
LM-1373	**Let's Encrypt ACME Certificates**: After certificate renewal, the old certificate may still be in use by the Virtual Service. The workarounds are to either: • Remove and re-add the Virtual Service certificate • Disable and re-enable the Virtual Service
LM-477	**GEO Downgrade**: When downgrading from a release that supports **more than 64 IPs per FQDN** to a

	release that only supports **up to 64 IPs per FQDN**, the GEO configuration may become corrupted if there is at least one FQDN in the configuration that contains more than 64 IP addresses. The corruption will likely be evidenced by errors in the UI/API when you list the FQDNs. To avoid this issue entirely, reduce the number of IPs per FQDN to 64 or less for all FQDNs defined *before* you downgrade. If you have already downgraded, you can switch back to the previous boot partition to go back to the newer release (which supports > 64 IPs per FQDN); you can then reduce the number of IPs as above and downgrade again. If neither of these options is possible, contact Progress Kemp Support who will consult with engineering on a solution to your issues.
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.
PD-19108, LM-127	**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, LM-127	**GEO**: Cannot configure GEO into partnering mode unless there is at least one FQDN already defined.
PD-18646, LM-133	**Certificate-Based Administrative Login**: Using a certificate that does not have a SAN attribute (that is, no Principal Name) results in a failed login attempt.
PD-18615, LM-134	**GEO**: No statistics (queries per second, and so on) are displayed for a site if the FQDN is configured to use the "All Available" Selection Criteria.
PD-18099, LM-136	**Client Certificates**: Authentication may be denied if multiple "Other names" are present in the client certificate.
PD-15872	**LDAP/Syslog**: StartTLS is not working when the **Server Certificate Validation** flag is enabled.
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 Virtual Service is dropped. Click the **Error Message** radio button in the UI and the Virtual Service 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 LM-142	**ESP Verify Bearer Header**: The LoadMaster does not return an error when an encrypted token is received and there is no SSL certificate assigned to the Virtual Service to decrypt the token.

PD-15172 LM-143	**ESP Verify Bearer Header**: Validation is not working when "Allowed Virtual Hosts" and "Allowed Virtual Directories" are blank on the Virtual Service.
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, and so on).
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 Virtual Service 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, contact Progress 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 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-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 UI.
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.