

LoadMaster 7.2.48.0 Release Notes

Generated on: 16 September 2024

Copyright

Visit the following page online to see Progress Software Corporation's current Product Documentation Copyright Notice/Trademark Legend: Product Documentation Copyright Notice & Trademarks | Progress

Table of Contents

Chapter 1: Introduction 5

Chapter 2: Supported LoadMaster Models 6

Chapter 3: New Features 8

LMOS Kernel Update 8

Security Vulnerabilities Closed 8

SSO Password Reset Notification 9

TCP SACK Support 9

Sharepoint 2019 Support & Skype for Business 2019 Support 9

10 Gb Interface Support on AWS Cloud 9

Chapter 4: Feature Enhancements 11

Surface MELA licensing error message descriptions 11

Licensing Workflows Simplified 11

Chapter 5: Change Notices 12

Single Upgrade Image 12

VMware vmxnet Network Interfaces No Longer Supported (Use vmxnet3) 12

Weak hmac-sha1 MAC Algorithm No Longer Supported 13

SPLA to MELA Conversion via Kemp 360 Central 13

Chapter 6: Issues Resolved. 14

Chapter 7: New Known Issues 18

Chapter 8: Existing Known Issues 20

1

Introduction

LMOS Version 7.2.48.0 is a feature and bug-fix update released in October 2019. Please read the sections below before installing or upgrading.

2

Supported LoadMaster Models

This release of LMOS is supported on the Hardware and Virtual platforms specific in the first two columns of the table below. *It is not supported and should not be installed on any of the hardware and software listed in the two columns at right.*

Supported Hardware Models	Supported Virtual Models	UNSUPPORTED Hardware Models	UNSUPPORTED Virtual Models
LM-X3	**VLM-200**	**LM-2000**	**VLM-100**
LM-X15	**VLM-2000**	**LM-2200**	**VLM-1000**
LM-X25	**VLM-3000**	**LM-2500**	
LM-X40	**VLM-5000**	**LM-2600**	
LM-2400	**VLM-10G**	**LM-3500**	
LM-3000	**VLM-GEO**	**LM-3600**	
LM-3400		**LM-5300**	
LM-4000		**LM-5500**	
LM-5000		**LM-Exchange**	
LM-5400		**LM-GEO**	
LM-5600			

Supported Hardware Models	Supported Virtual Models	UNSUPPORTED Hardware Models	UNSUPPORTED Virtual Models
LM-8000			
LM-8020			
LM-8020M			
Bare Metal			

If your model number is not listed above, please see the list of End of Life models.

3

New Features

The following new features have been implemented.

Related Links

- LMOS Kernel Update
- Security Vulnerabilities Closed
- SSO Password Reset Notification
- TCP SACK Support
- Sharepoint 2019 Support & Skype for Business 2019 Support
- 10 Gb Interface Support on AWS Cloud

LMOS Kernel Update

The LMOS kernel has been updated to version 4.14.137 of the Linux kernel.

Security Vulnerabilities Closed

The following security vulnerabilities have been verified as closed with the new kernel update:

- CVE-2019-10639
- CVE-2019-11477

- CVE-2019-11478
- CVE-2019-11479

SSO Password Reset Notification

A new option has been added to the ESP options for Virtual Services that allows you to specify that the user's password expiration date will be checked whenever a user logs in through an SSO form. If the user's password will expire within a configurable number of days, a warning is displayed to the user along with a link that will allow them to update their password. This new ESP option, **User Password Expiry Warning**, can only be enabled once the **User Password Change URL** setting is enabled. You can also set the number of days before password expiry that the warning will begin to appear; the default is 15 days. Please also see the New Known Issues section.

TCP SACK Support

In previous releases, TCP Selective Acknowledgement (aka: TCP SACK) could be enabled on LoadMaster only by logging into the OS. With this release, you can now control the TCP SACK setting in the UI and via the API. This global setting is located in the UI under **System Configuration > Logging Options > System Log Files > Debug Options**. Note that TCP SACK is a global setting (i.e., it affects all TCP traffic) and is disabled by default. If you change the default setting, your change will persist across future LoadMaster reboots.

Sharepoint 2019 Support & Skype for Business 2019 Support

New Kemp-approved LoadMaster Application Templates are now available from the Kemp website for **Sharepoint 2019** and **Skype for Business 2019**. See the **Templates** section at right and click on the **Microsoft** link.

10 Gb Interface Support on AWS Cloud

Virtual LoadMasters deployed within the AWS Cloud now support 10 Gbps throughput interfaces. This support comes with a few limitations:

- Link on the single logical ENA interface cannot be detected through the OS, so 'No Link' will be displayed when the interface status is queried via the API or displayed in the UI.
- Interface Graphs for 10 GB interfaces on the statistics page are displayed incorrectly. This will be addressed in a future release.

If you upgrade from a release prior to 7.2.48 to 7.2.48 or a later release and your AWS VM is running a virtual machine instance type that *does not* support 10 GB interfaces (e.g., "m4.10xlarge"), you must convert the VM to a machine type that supports 10 GB interfaces (e.g., "m4.16xlarge) to enable 10 GB interfaces on LoadMaster. Following these steps:

- Shut down LoadMaster using the LMOS UI or API.
- Enable ENA driver support on the AWS virtual machine:

  ```
  aws ec2 modify-instance-attribute --instance-id instanceID --ena-support
  ```

- Change the AWS virtual machine instance type to one that supports the ENA 10 GB driver (e.g., m4.16xlarge) using the AWS UI.
- Start the LoadMaster VM.

4

Feature Enhancements

The following feature enhancements are included in this release.

Related Links

- Surface MELA licensing error message descriptions
- Licensing Workflows Simplified

Surface MELA licensing error message descriptions

Error message reporting when requesting a license from an instance of Kemp 360 Central running firmware Version 2.4 (and above) has been improved.

Licensing Workflows Simplified

Licensing workflows have been modified and simplified for a better user experience, and so that the API and UI workflows are more consistent.

5

Change Notices

This release includes the following modification to existing behavior that may require changes to procedures and/or scripts currently in use within your organization.

Related Links

- Single Upgrade Image
- VMware vmxnet Network Interfaces No Longer Supported (Use vmxnet3)
- Weak hmac-sha1 MAC Algorithm No Longer Supported
- SPLA to MELA Conversion via Kemp 360 Central

Single Upgrade Image

In previous releases, there were 3 upgrade images: one for AWS Cloud, one for Azure Cloud, and one for all other platforms. Starting with 7.2.48.0, there is now a single upgrade image for all platforms.

VMware vmxnet Network Interfaces No Longer Supported (Use vmxnet3)

Support for the VMware legacy *vmxnet* network interface driver is removed from Loadmaster starting with this release and will no longer be available. The vmxnet network interface dates from ESXi 3.5 and earlier releases, and does not support many of the feature available on modern networks.

Instead, customers with existing VMware deployments that use *vmxnet* interfaces should modify the VMware configuration of the LoadMaster to use the latest *vmxnet3* network interfaces *before* upgrading to LMOS 7.2.48. This will require a LoadMaster reboot.

For an overview of VMware drivers and versions, please see this VMware article.

Weak hmac-sha1 MAC Algorithm No Longer Supported

SSH support for the weak MAC algorithm **hmac-sha1** has been removed with this release. This may result is some older versions of SSH no longer working with LoadMaster.

SPLA to MELA Conversion via Kemp 360 Central

A new workflow has been implemented that facilitates the conversion of a SPLA-licensed LoadMaster to Metered Licensing (or MELA). This process leverages improvements in the Kemp 360 Central Version 2.4 license activation process, so that re-provisioning of the LoadMaster and its configuration is no longer required as in the past. To request assistance with this conversion workflow please contact Kemp Sales.

As part of this change, **Kemp 360 Central** will now appear as a licensing choice when first installing LoadMaster 7.2.48.0 (and later) versions.

- If you choose this option and the Kemp 360 Central from which you attempt to obtain a license is running Version 2.4 (or later), then you will only be able to license from Kemp 360 Central if the available license pool on Kemp 360 Central includes a license that is appropriate for the LoadMaster image you are installing. If not, then Kemp 360 Central will return the following: “WARNING: No License configured for LM SKU *name*”.
- If you choose this option and the Kemp 360 Central from which you attempt to obtain a license is running a firmware version *earlier* than Version 2.4, then you may successfully receive and activate a license that is not appropriate for the LoadMaster image you are installing. If you observe that Kemp 360 Central is not displaying the newly added device’s configuration, then this may be the issue. Please call Kemp Support for assistance.

6

Issues Resolved

The following issues have been resolved in this release.

PD-13828	**IPv6**: Under certain circumstances, specifying a Real Server using an FQDN (rather than a hostname or IP address) can result in the FQDN resolving to an invalid IPv6 address. This issue has been fixed.
PD-13816	**GEO**: In previous releases, the DNS server returns NXDOMAIN or NODATA when there are disabled IPv4 or IPv6 records (i.e., sites) present in the configuration. The DNS server behavior has been modified so that it returns NOERROR in these cases.
PD-13808	**Licensing API**: For consistency, the *aslactivate()* and *alsilicense()* routines will now accept either *licensetypeid* or *lic_type_id* as the parameter specifying the license type.
PD-13802	**SPLA Licensing**: Fixed an issue that could cause several spurious virtual services to appear after a fresh install.
PD-13794	**Memory Consumption on Upgrade to 7.2.47**: Upgrading a LoadMaster with over 4GB of memory to version 7.2.47 (only), could result in a significant increase in system memory usage on large configurations (many unique Real Server IP/port combinations). This issue has been fixed.
PD-13785	**User Interface**: Fixed an issue that caused spurious text to appear at the bottom of the **Certificates & Security > Remote Access** UI when the **Admin Login Method** was modified.
PD-13780	**HTTP/2**: An issue that caused embedded videos to fail to load properly via HTTP/2 virtual services has been fixed.
PD-13776	**User Interface LDAP Login**: Fixed an issue where access is denied by some LDAP servers when specifying permitted groups.

PD-137 52	**User Interface**: Modified the UI so that the date/time format on the **Home** page and the **Update License** page are the same.
PD-137 50	**WAF API**: Fixed an issue with the *maninstallwafrules()* API returning 'Unknown Command' when the API was executed successfully.
PD-137 49	**Security / SSH**: Support for the weak MAC algorithm **hmac-sha1** has been removed with this release. This may result is some older versions of SSH no longer working with LoadMaster.
PD-137 39	**User Interface Security**: Fixed an issue where LoadMaster was re-generating the default UI certificates after a reboot.
PD-137 27	**WAF Rules / User Interface Resiliency**: In LMOS version 7.2.47, if the download and installation of WAF rules fails on LoadMaster due to corruption, this failure could contribute to the exhaustion of available temporary storage, which would cause the UI to become unavailable. This issue has been fixed.
PD-137 20	**HTTP/2**: Fixed an issue that, when HTTP/2 is enabled on a SubVS, caused only the HTTP/2 response code and *not* the associated error message text to be returned to the client.
PD-137 12	**UI Cipher Sets**: Modified the UI so that Cipher Set can be named using both plus (+) and minus (-) characters.
PD-136 72	**Application Template Import**: Fixed an issue where you could not import a template containing SubVSs with Basic Authentication enabled on the Client side.
PD-136 69	**License Expiration**: Fixed an issue where LoadMaster services were not being disabled after the system license and applicable grace period had expired.
PD-136 68	**UI Client Certificate Authentication**: Changes were made in 7.2.46 that caused client certificate authentication for the UI to fail. This issue has been fixed.
PD-136 64	**VMware Tools & VM Workstation**: Fixed an issue with the VMWare Tools Add-on that caused an error to be displayed when deploying a LoadMaster in VM Workstation.
PD-136 32	**Secure Flag in Cookies**: In previous releases, the Secure flag in HTTP cookies is only set if the user adds a specific content rule to set it. With this release, the Secure flag is always set when Active Cookie persistence is selected for an HTTPS virtual service.
PD-135 83	**FIPS Ciphers**: Fixed the list of FIPS ciphers in the UI so that it is correct.
PD-135 61	**Health Checking**: When using a POST HTTP health check, the POST data is being sent as URL-encoded text instead of being sent as raw data. This issue has been fixed.
PD-135 51	**Single Sign On (SSO)**: On LMOS 7.2.47.1 only, when a virtual service configuration uses NTLM + KCD for user authentication, the connection will close and force the user to re-authenticate. The LoadMaster will also log segfault errors. This issue has been fixed.
PD-135 40	**VLANs on Bonded Interfaces**: In previous releases, when adding or deleting VLANs on a bonded interface, connectivity on that VLAN will be lost during the operation. With this release, you can add and delete VLANs to a bonded interface without losing connectivity on the VLAN.
PD-135 15	**Sorry Server**: Adding a 'sorry server' to an HTTPS straight through virtual service does not work. This issue has been fixed.
PD-135	**GEO**: Modified how the view configuration file is generated to prevent intermittent response issues seen

11	while using GEO with a Zone Name specified.
PD-135 07	**SAML**: Fixed an issue where the Subject Name Identifier in the SAML response was not being handled properly, resulting in errors.
PD-135 00	**SSO**: A colon character (:) can now be included in the **Allowed Virtual Hosts** value via the API and in the UI under a virtual service's **ESP Options**.
PD-134 98	**HTTP/2**: In previous releases, an SSL accelerated virtual service would not work properly after changing the service type from **HTTP-HTTP/2-HTTPS** to **HTTP/2 Pass-through**. This issue has been fixed.
PD-134 96	**Powershell API**: A new cmdlet, *Get-SSODomainQuerySession*, is provided to fetch SSO domain sessions.
PD-134 32	**MELA Licensing**: In previous releases, when a MELA license obtained from Kemp 360 Central expires, you cannot re-license the Loadmaster with the same license type. With this release, this restriction has been removed.
PD-134 31	**Licensing**: In previous releases, it was possible to license a Free LoadMaster via offline licensing and disable call home. This has been changed so that a Free LoadMaster can only be licensed online. In addition, call home is enabled by default and cannot be disabled.
PD-134 01	**Memory Exhaustion:** In previous releases, in a LoadMaster with a RAM size of 8GB or less it was possible that the system would run out of memory if there were a large number of long lived SSL connections. With this release measures have been implemented to prevent the system from running out of memory.
PD-134 00	**SSO**: In previous releases, when **Failed Login Attempts** is set to '1', a user will not get blocked until after 2 failed login attempts. This issue has been fixed.
PD-133 76	**MELA Licensing**: In previous releases, a LoadMaster deployed in Azure did not send its public IP to Kemp 360 Central during licensing, and so Kemp 360 Central could not communicate with it. This issue has been fixed.
PD-132 76	**Statistics**: Fixed issues observed on some platforms where the UI and/or API were reporting differing, incorrect, or invalid values.
PD-131 26	**GEO**: In previous releases, the DNS server returns NXDOMAIN for a query on the second level of a child domain. With this release, the NOERROR status is returned for a DNS query sent on any level of a child domain.
PD-130 65	**Interface Bonding**: (LoadMaster X15 only) Issues seen when bonding interfaces between certain Cisco switches have been fixed.
PD-130 53	**SSO**: In previous releases, clicking the 'Kill All' button when viewing the open sessions for one SSO domain also kills all open sessions in all other SSO domains. With this release, only the open sessions associated with the domain being displayed are killed.
PD-130 45	**SAML**: In previous releases, if there are many SAML based sessions open when trying to view open sessions, the WUI does not display the sessions and instead a segmentation fault appears in the logs. This issue has been fixed.
PD-129 62	**Virtual Service Names**: In previous releases, it was possible to begin the name of a virtual service with a number or a special character. This is no longer permitted.
PD-127	**SSO**: API (and UI) response times for retrieving/displaying a large number of SSO open sessions has been

67	improved so that most queries complete in under 1 second.
PD-12668	**ActiveSync Virtual Services**: Connectivity Issues with ActiveSync Virtual Services may be observed at high traffic volumes. Previously, under high load and thousands of SSO sessions, the LM memory utilization would grow until it ran out of memory.Now, there may be thousands of SSO sessions and the LM memory will remain steady.
PD-12384	**KCD Server Authentication**: Modified ticket handling to improve response times.
PD-12068	**Clustering & Memory Management**: Addressed issues causing shared memory corruption when the cluster type is **Remote LM** and the configuration contains a large number of virtual services.
PD-11737	**SAML & KCD**: In previous releases, SAML + KCD configurations were reported to experience high CPU usage and slow response times, causing interruptions in client traffic. Improvements to KCD authentication have been made to lower CPU utilization and provide faster response times.

7

New Known Issues

The following known issues appear in these *Release Notes* for the first time.

PD-14100	**ESP SSO**: After login through the LoadMaster Single Sign On Outlook Web Access forms, the user is immediately logged out. This issue will be addressed in a future release.
PD-14054	**Virtual Services with Wildcard URLs**:Traffic running through a Virtual Service with a wildcard URL may cause the LoadMaster to reboot. This issue will be addressed in a future release.
PD-14047	**UDP Virtual Services**: UDP services on port 53 that use the Layer 7 non-transparent mode do not work correctly. This issue will be addressed in a future release.
PD-14046	**Bare Metal**: On certain bare metal LoadMasters, network interfaces no longer work after upgrade to 7.2.48. This issue will be addressed in a future release.
PD-14038	**API**: The PowerShell API "Remove-SplaInstance" is broken due to changes in the RESTful API "kill_spla_instance" response. This issue will be addressed in a future release.
PD-14036	**API**: The PowerShell API "Get-LicenseType" is broken due to changes in the RESTful API "alsilicensetypes" response. This issue will be addressed in a future release.
PD-14028	**Licensing**: After upgrade to 7.2.48, Trial LoadMasters have the 'Offline Licensing' option grayed out (non-selectable) on the 'Update License' page. This issue will be addressed in a future release.
PD-13904	**SSO**: Password expiry notifications do not currently work with Forms Based Authentication (FBA) enabled on the server side. This issue will be addressed in a future release.
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.

8

Existing Known Issues

The following known issues appeared in the *Release Notes* for the previous 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-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	**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-976	**GEO**: DNS TCP requests from unknown sources are not supported.

5	
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.