LoadMaster

Release Notes

UPDATED: 23 March 2018

Copyright Notices

Table of Contents

1 Software Release Notes Introduction

This document describes the features in the current and previous LoadMaster releases.

We recommend you fully back up the LoadMaster configuration before upgrading the software. Instructions for backing up the LoadMaster are described in within the documentation which can be found at http://kemptechnologies.com/documentation.

Installation of this software and reloading of the configuration may take up to five minutes, or possibly more, during which time the LoadMaster being upgraded is unavailable to carry traffic.

1.1 Pre-requisites

The following are recommendations for upgrading the software:

- The person undertaking the upgrade should be a network administrator or someone with equivalent knowledge.
- In case of issues restoring backup configurations, configuring LoadMaster or other maintenance issues, please refer to the LoadMaster documentation which can be found at http://kemptechnologies.com/documentation.

1.2 Support

If there are problems loading the software release, please contact KEMP support staff and a KEMP support Engineer will get in touch with you promptly: http://kemptechnologies.com/load-balancing-support/kemp-support

1.3 Compatible Products

- LM-X15
- LM-X3
- LM-2400
- LM-2600
- LM-3600
- LM-5300
- LM-5400
- LM-5000
- LM-5600
- LM-8000
- LM-8020 (supported on version 7.1-30 and above)
- LM-3000
- LM-4000
- VLM-1000
- VLM-2000
- VLM-5000
- VLM-DR
- LM for UCS B Series
- LM for UCS C Series
- LM for Oracle Sun x86 servers
- LM for HP ProLiant servers
- LoadMaster for Fujitsu Primergy
- LoadMaster for Dell R-Series

- LM-R320
- VLM-100
- VLM-200
- VLM-Exchange
- LoadMaster for AWS
- LoadMaster for Azure

2 Release 7.2.41.2

Refer to the sections below for details about firmware version 7.2.41.2. This was released on 23rd March 2018.

2.1 7.2.41.2 - New Features

The following feature was added to the 7.2.41.2 release:

- Added support for the new LM-X series of LoadMaster hardware.

2.2 7.2.41.2 - Issues Resolved

PD-10980	Previously, a critical vulnerability in the LoadMaster Operating System (LMOS) related to Session Management could allow an unauthorized, remote attacker to bypass security protections, gain system privileges, and execute elevated commands such as **ls**, **ps**, **cat**, and so on, thereby compromising the system. Through this remote execution, in certain cases, exposure of sensitive system data such as certificates, private keys, and other information may be possible. Now, this vulnerability has been mitigated against with more stringent security checks. Further information can be found here: Mitigation For Remote Access Execution Vulnerability.

2.3 7.2.41.2 - Known Issues

PD-10139	**Using WAF with ESP and KCD is not supported with Microsoft Exchange 2010.**
PD-9765	GEO does not support DNS TCP requests from unknown sources.
PD-8697	Some users are experiencing issues detecting the partition when using the Hardware Security Module (HSM).
PD-9375	Microsoft Office files in SharePoint do not work in Firefox and Chrome when using SAML authentication.
PD-9649	Some users are experiencing a SAML error "Could not base64 decode the SAMLResp".
PD-9821	Some high memory usage has been observed.
PD-10129	There is a discrepancy in validation between global-level connection timeout and Virtual Service-level timeout.
PD-10131	There are some problems attaching files in SharePoint when using WAF with **Process Responses** enabled and Kerberos Constrained Delegation (KCD).

PD-10149	It has been observed that Alternative Domain selection and handling is not always reliable. While an Alternative Domain may be selected appropriately, the Virtual Service association is not always consistent. As a result, Form Based Authentication (FBA) on the server side is not triggered when expected. Furthermore, some characters are not permitted to be included in the server side FBA post to the Real Server.
PD-10159	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-10188	When adding a Real Server to a Virtual Service or SubVS on a Safari browser, the list of available Real Servers is not available.
PD-10197	Cluster Virtual Service and Real Server home page statistics are reported incorrectly.
PD-10207	The ESP LDAP logs need to be enhanced.
PD-10259	When under load, WAF does not read all of the Real Server responses and closes the connection prematurely.
PD-10332	When you try to add a duplicate VLAN ID/VXLAN ID, text saying "Duplicate VLAN id/VXLAN id Cache-Control: no-cache" appears in the WUI.
PD-10381	Removing **Application Generic** rule sets from the Virtual Service causes WAF misconfiguration.
PD-10445	Some websites do not work when the **WAF Process Responses** option is enabled.
PD-10455	Amazon Web Services (AWS) cannot use the admin certificate after a reboot.
PD-10474	A SNORT rule is triggering a false positive in certain scenarios.
PD-10478	Custom SSO image set is not displaying in the **SSO Image Set** drop-down list after the ESP SSO configuration is restored from a backup.
PD-10488	Occasionally WAF is getting stopped with an "errno 24" error.
PD-10525	Some users are experiencing WAF read errors when connections are closing.
PD-10538	Cannot create body rules when single quotes are in separate capture groups.
PD-10545	Virtual LoadMasters become inaccessible on Azure cloud when the WUI is moved to NIC-1.
PD-10572	The extended log view fails when the selected range is in different years.
PD-10584	There are some SAML User Principal Name (UPN) and SAM-Account-Name interaction issues.
PD-10590	Automatic WAF rule downloads are not working on the second HA node even if it is active.
PD-10616	When WAF **Process Responses** is enabled, the response is cut.

PD-10627	There are issues when replacing clustered nodes.
PD-10702	There are spurious KCD credentials expired log messages.
PD-10586	If a GEO FQDN is configured with **All Available** as the **Selection Criteria**, IPs are returned even if the cluster is disabled.
PD-10155	An issue with configuration corruption is causing some GEO features to not function.
PD-8725	**Proximity** and **Location Based** scheduling do not work with IPv6 source addresses.
PD-8853	**Location Based** failover does not work as expected.
PD-7156	The VSIndex parameter is missing in some API commands.
PD-9476	There is no RESTful API command to get/list the installed custom rule data files.
PD-9507	Unable to add an SDN controller using the RESTful API/WUI in a specific scenario.
PD-9553	There is no API command to disable secure NTP mode.
PD-9816	There is an API command to list individual rules in a ruleset, but there is no command to list the available rulesets themselves.
PD-9947	Virtual Services/Real Servers can report as "Up" in the API even if SubVSs are disabled.
PD-10363	The PowerShell API is missing the **ServerFbaPath** and **ServerFBAPost** parameters.
PD-10421	Setting options for the syslog server settings multiple times for different levels using the API causes events to repeat.
PD-10490	The **vsremovewafrule** RESTful API command does not allow multiple rules to be removed.
PD-10577	Some API calls are failing due to NULL pointers.
PD-10598	There is no PowerShell API parameter to modify the **IdP Certificate Match** option.

3 Release 7.2.41.1

Refer to the sections below for details about firmware version 7.2.41.1. This was released on 21st February 2018.

3.1 7.2.41.1 - Feature Enhancements

- Previously, there was no specific SubVS information detailed in the logs when a failure occurred.
  Now, the logs are updated with Virtual Service and SubVS names when a failure occurs.
- Previously, Virtual LoadMaster (VLM) cloud instances only listened for port 8444 on eth0.
  Now, there is an option to listen on all interfaces.
- The LoadMaster Operating System (LMOS) Linux kernal was upgraded from linux-4.4.32 to linux-4.9.58 to improve performance and latency issues observed in previous releases.
- Previously, text/XML and application/JSON content types were supported with the **Inspect HTML POST Request Content** feature.
  Now, the new **Enable Other Content Types** option enables the selection of all content types or specified content types.
- Previously, the User Agent String was not present in the log files.
  Now, the new **Include User Agent Header in User Logs** option on the **L7 Configuration** screen enables User Agent String information to be printed in the logs.
- Previously, SSO manager logs were collected under the ssomgr logs option in the **Extended Log Files** section of the LoadMaster WUI.
  Now, the SSO manager logs (with levelled debug logging) are collected and managed in the system log file. This improves managing logs centrally.
- Previously, there was no indication of where to find the LDAP endpoint from the SSO domain configuration, LDAP WUI auth, and Real Server health check.
  Now, a modify LDAP configuration button is in the manage SSO configuration, WUI auth LDAP setting, and Virtual Service Real Server health check.
- Previously, the default value for the additional L7 headers field was Legacy (X-ClientSide).
  Now, the default value for the additional L7 headers field is X-Forwarded-For.
- Previously, the default value for the **100-Continue-Handling** field was **RFC-2616 Compliant**.
  Now, the default value for the **100-Continue-Handling** field is **RFC-7231 Compliant**.
- Previously, the **L7 Connection Drain Time (secs)** field was not available next to the **Drop at Drain Time End** field.
  Now, the **L7 Connection Drain Time (secs)** field is underneath the **Drop at Drain Time End** field.
- Previously, the default global setting for Enable Non-Local Real Servers was disabled.
  Now, the default global setting for Enable Non-Local Real Servers is enabled.
- Previously, on VLMs there were **ttyS0: ioctl: Input/output error** messages in the system logs.
  Now, there are no respawn or ttys0-related messages in syslog.
- Previously, GMT offset settings were on top of the **Set Timezone** drop-down list options.
  Now, the GMT offset settings are on the bottom of the **Set Timezone** drop-down list options.

- Previously, the bonding option was available in the WUI and RESTful API for cloud platforms like AWS and Azure, but it was not a supported feature.
  Now, the bonding option is disabled and removed from the WUI and RESTful API for cloud platforms.
- Previously, when the user was unable to add a Virtual Service or SubVS, the error message displayed in the WUI was unclear.
  Now, the error message is better and it advises that the LoadMaster is under-resourced and therefore a new Virtual Service or SubVS cannot be added.
- Previously, connectivity broke when moving the default gateway to another interface.
  Now, you can move the default gateway to another interface without affecting connectivity.
- Previously, the WUI displayed inappropriate warning messages when a user attempted to configure an IP address which is already configured on another interface.
  Now, the WUI displays an updated warning message informing that the IP address is already configured on another interface.
- The **System Log Files** screen now shows the percentage used/free in relation to log partitions.
- Previously, the firmware update license error message did not have enough details and caused confusion.
  Now, clear and concise feedback about why the failure has happened, and a link to a Help Center article, is provided.
- Previously, there were platform-specific Application Program Interface (API) commands, for example, for Azure there is a **getazurehaparams** command and for AWS there is a **getawshaparams** command.
  Now, there is a common API command called **getCloudHaParams** for querying HA parameters on all cloud platforms.

3.2 7.2.41.1 - Issues Resolved

PD-9764	Previously, IPsec had connectivity issues to Azure for LoadMaster firmware version 7.2.38.2 and above. Now, IPsec successfully connects to Azure.
PD-9944	Previously, the WUI allowed up to 208 characters in the **Header Field**, **Match String**, **Value of Header Field to be Added**, **Modified URL**, and **Value of Header Field to be replaced** fields when creating and modifying content rules. Now, this limit is 255 characters in the WUI and RESTful API.
PD-9975	Previously, there were no logs when an LDAP AAA test user failed. Now, there are logs when an LDAP AAA test user fails.
PD-10039	Previously, the HTTP/2 stack had issues with features like shopping carts with browsers other than Internet Explorer. Now, HTTP/2 works with Chrome, Firefox, and Internet Explorer.

PD-10040	Previously, icb_alloc logs can be seen if the Web Application Firewall (WAF) is enabled and chunked data is received. Now, icb_alloc messages do not appear in logs.
PD-10042	Previously, WAF statistics did not get cleared/reset on Virtual Service deletion. Now, WAF statistics get cleared (set to 0) on Virtual Service deletion.
PD-10051	Previously, LoadMaster activation failed when re-licensing the LoadMaster multiple times. Now, a reboot is required after each re-license.
PD-10071	Previously, the libxml2 GNOME XML library was installed. Now, the library has been updated to libxml2-2.9.5.
PD-10083	Previously, the LoadMaster did not return a complete list of Virtual Services and Real Servers when queried using a MIB browser or **smtpwalk** command. Now, the LoadMaster returns a complete list of Virtual Services and Real Servers configured when queried using a MIB browser or **smtpwalk** command.
PD-10086	Previously, the WUI displayed inappropriate warning messages when attempting to configure an IP address which is already configured on any interface. Now, the WUI displays an updated warning message if you attempt to configure an IP address which is already configured on any interface.
PD-10141	Previously, the check interval time was stored incorrectly in the configuration file and caused unwanted LoadMaster FIN ACK traffic.
PD-10142	Previously, the master LoadMaster did not send uCAP packets every second. It randomly missed one or more packets. Now, this bug is fixed and both the WUI and configuration shows similar check interval with no unwanted traffic.
PD-10204	Previously, the replace certificate in LoadMaster WUI workflow had a minor error and did not allow the user to replace the certificate. Now, the replace certificate workflow has been improved and the user can replace a certificate using the WUI.
PD-10205	Previously, underscores, dashes, and square brackets were not allowed in the Form Authentication Path field in the WUI. Now, underscores, dashes, and square brackets are allowed in the Form Authentication Path field in the WUI.
PD-10235	Previously, log rotation for the adaptive.log file did not work on LoadMasters without the SDN add-on. Now, log rotation works for the adaptive.log file on LoadMasters without the SDN add-on.

PD-10239	Previously, the Pre-Shared Key (PSK) was unencrypted in backup files. Now, the PSK is encrypted. **Note:** If upgrading the LoadMaster firmware to 7.2.41.1, ensure to re-enter the PSK to ensure it is encrypted. If you do not do this, the VPN still works, but the new security measure does not take effect until the PSK is re-saved.
PD-10245	Previously, when trying to access the connection, security, and user extended log files - the previous days logs were grayed out and you could not view them. Now, the **Extended Log Files** screen includes options to select by date, files, and filter. Also, when viewing Edge Security Pack (ESP) logs, selecting the next date includes logs from the previous date.
PD-10255	Previously, the default value for the **Strict Transport Security Header** field was **Add the Strict Transport Security Header - include subdomains**. Now, the default value for the **Strict Transport Security Header** field is **Don't add the Strict Transport Security Header**.
PD-10345	Previously, connectivity on Link Aggregation Control Protocol (LACP) bonded interface did not work with some switch hardware. Now, LACP bonded interfaces are activated quickly and connectivity works on this port as expected.
PD-10353	Previously, in the warning logs on Federal Information Processing Standards (FIPS) boxes, there were multiple instances of a log message **FIPS selftest completed successfully. Using FIPS mode.** Now, this message no longer repeats. This shortens the logs length for download and parsing.
PD-10354	Previously, bare metal ISO installations would sometimes obtain an invalid value for the serial number. Now, the serial number obtains successfully.
PD-10355	Previously, when using SAML client authentication and a user opens a second tab, the user received an Access Denied error message. Now, the user is redirected to the federated server login page (for example, the Active Directory Federation Services (AD FS) login). KEMP recommends that the user continues to use the latest tab opened for login access. Otherwise, the authentication may get confused due to temporary cookie use and SAML Response ID matching may fail.
PD-10361	Previously, the LM-4000 model had stability issues on LoadMaster firmware version 7.2.36.1 with certain traffic. Now, a fix has been implemented to improve stability.

PD-10368	Previously, the RADIUS server password could not be set using the API. Now, the RADIUS server password can be set using the API.
PD-10374	Previously, when using the **Client Certificate** authentication mode, the user credentials for the SSO domain health checks over LDAP (LDAPS and StartTLS), were in plain text and visible in a protocol capture trace. Now, when using the **Client Certificate** authentication mode, the SSO domain health checks use StartTLS and therefore the user credentials are no longer visible in a protocol capture trace.
PD-10393	Previously, the signature verification in the case of a trusted certificate and intermediate certificate did not work. The certificate in the response must match the certificate assigned in the SAML SSO domain. Now, with the IDP Certificate Match option, both pre-7.2.40 and post-7.2.40 behavior allowing configuration for strict matching of the certificate.
PD-10433	Previously, active/backup bonding did not work when the cable was plugged out from the active interface. Now, active/backup bonding works correctly when the cable is plugged out from the active interface and the connection shifts to the backup interface.
PD-10448	Previously, log rotation did not work when the rotation file name already existed. Now, log rotation is working properly.
PD-10461	Updated the OpenSSL version from 1.02k-fips to 1.0.2n-fips.
PD-10477	Previously, adding clients to an SSO image set with more than 32 special characters ('%') caused L7d to crash. Now, this bug is fixed and nearly 256 special characters are allowed in the client SSO image set input file.
PD-10486	Previously, WAF did not block all POST attack requests when multiple content-types are set for the **Enable Other Content Types** option. Now, WAF blocks all POST attack requests when multiple content-types are set for the **Enable Other Content Types** option.
PD-10514	Previously, the copyright date in the LoadMaster was 2017. Now, the copyright date is 2018.
PD-10530	Previously, unwanted error messages appeared when navigating to the Default Gateway. Now, no error message appears when navigating to the Default Gateway.
PD-10637	Previously, use of the configured port for the target OCSP server and SSL responses from the server were handled incorrectly. Now, the port configured for the OCSP server is used correctly per the configuration

	setting on the LoadMaster. SSL responses are also handled correctly.
PD-10096	Previously, on occasions the GEO zone serial is not refreshed causing a spurious "Zone may fail to transfer to slaves" log message. Now, the log level for these messages have been changed from ERROR to INFO. These messages do not affect functionality.
PD-10115	Previously, if an FQDN with a wildcard and another FQDN belonging to the same domain is configured, in some scenarios GEO can pick up the wildcard FQDN instead of the correct FQDN. Now, GEO picks up the correct FQDN even if the configuration has a wildcard FQDN.
PD-10473	Previously, GEO returns sites that are down if the **Selection Criteria** is set to **All Available**. Now, only sites with a status of "up" are returned.
PD-9525	Previously, the **showfqdn** API command displayed the **Failtime** value in seconds, but it is set in minutes. Now, the **showfqdn** API command displays the **Failtime** value in minutes.
PD-9785	Previously, running an Azure PowerShell command after calling any LoadMaster PowerShell command with a self-signed certificate returned an error. Now, Azure PowerShell commands work as expected, even when running after executing any LoadMaster PowerShell command with a self-signed certificate.
PD-10043	Previously, there was no RESTful API command to get the WAF logging format and remote logging details. Now, WAF logging format and remote logging details can be retrieved by running the **getwafsettings** RESTful API command.
PD-10076	Previously, **Credential** was a mandatory parameter for the **Get-LicenseType** PowerShell command. Now, **Credential** is an optional parameter for the **Get-LicenseType** PowerShell command.
PD-9539	Previously, the **New-GeoCluster** command returned an invalid error, when you try to add a GEO cluster that already exists with the same name and IP address. Now, for the same scenario, the **New-GeoCluster** command returns a proper error message: **Cluster already defined. Name/IP must be unique**.
PD-9570	Previously, the **removecountry** API command error message had a typo (**countries** was spelled **counries**). Now, the typo in the **removecountry** API command error message is fixed.
PD-9572	Previously, the **showcluster** and **showfqdn** API commands displayed location

	parameter values in degrees, but the **showip** API command displayed the values in seconds. Now, the **showfqdn**, **listfqdns**, **showip**, **listops**, **showcluster**, and **listclusters** API commands display the values in seconds.

3.3 7.2.41.1 - Known Issues

PD-10980	A critical vulnerability in the LoadMaster Operating System (LMOS) related to Session Management could allow an unauthorized, remote attacker to bypass security protections, gain system privileges, and execute elevated commands such as **ls**, **ps**, **cat**, and so on, thereby compromising the system. Through this remote execution, in certain cases, exposure of sensitive system data such as certificates, private keys, and other information may be possible. Further information can be found here: Mitigation For Remote Access Execution Vulnerability.
PD-10139	**Using WAF with ESP and KCD is not supported with Microsoft Exchange 2010.**
PD-9765	GEO does not support DNS TCP requests from unknown sources.
PD-8697	Some users are experiencing issues detecting the partition when using the Hardware Security Module (HSM).
PD-9375	Microsoft Office files in SharePoint do not work in Firefox and Chrome when using SAML authentication.
PD-9649	Some users are experiencing a SAML error "Could not base64 decode the SAMLResp".
PD-9821	Some high memory usage has been observed.
PD-10129	There is a discrepancy in validation between global-level connection timeout and Virtual Service-level timeout.
PD-10131	There are some problems attaching files in SharePoint when using WAF with **Process Responses** enabled and Kerberos Constrained Delegation (KCD).
PD-10149	It has been observed that Alternative Domain selection and handling is not always reliable. While an Alternative Domain may be selected appropriately, the Virtual Service association is not always consistent. As a result, Form Based Authentication (FBA) on the server side is not triggered when expected. Furthermore, some characters are not permitted to be included in the server side FBA post to the Real Server.
PD-10159	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-10188	When adding a Real Server to a Virtual Service or SubVS on a Safari browser, the list of

	available Real Servers is not available.
PD-10197	Cluster Virtual Service and Real Server home page statistics are reported incorrectly.
PD-10207	The ESP LDAP logs need to be enhanced.
PD-10259	When under load, WAF does not read all of the Real Server responses and closes the connection prematurely.
PD-10332	When you try to add a duplicate VLAN ID/VXLAN ID, text saying "Duplicate VLAN id/VXLAN id Cache-Control: no-cache" appears in the WUI.
PD-10381	Removing **Application Generic** rule sets from the Virtual Service causes WAF misconfiguration.
PD-10445	Some websites do not work when the **WAF Process Responses** option is enabled.
PD-10455	Amazon Web Services (AWS) cannot use the admin certificate after a reboot.
PD-10474	A SNORT rule is triggering a false positive in certain scenarios.
PD-10478	Custom SSO image set is not displaying in the **SSO Image Set** drop-down list after the ESP SSO configuration is restored from a backup.
PD-10488	Occasionally WAF is getting stopped with an "errno 24" error.
PD-10525	Some users are experiencing WAF read errors when connections are closing.
PD-10538	Cannot create body rules when single quotes are in separate capture groups.
PD-10545	Virtual LoadMasters become inaccessible on Azure cloud when the WUI is moved to NIC-1.
PD-10572	The extended log view fails when the selected range is in different years.
PD-10584	There are some SAML User Principal Name (UPN) and SAM-Account-Name interaction issues.
PD-10590	Automatic WAF rule downloads are not working on the second HA node even if it is active.
PD-10616	When WAF **Process Responses** is enabled, the response is cut.
PD-10627	There are issues when replacing clustered nodes.
PD-10702	There are spurious KCD credentials expired log messages.
PD-10586	If a GEO FQDN is configured with **All Available** as the **Selection Criteria**, IPs are returned even if the cluster is disabled.
PD-10155	An issue with configuration corruption is causing some GEO features to not function.
PD-8725	**Proximity** and **Location Based** scheduling do not work with IPv6 source addresses.

PD-8853	**Location Based** failover does not work as expected.
PD-7156	The VSIndex parameter is missing in some API commands.
PD-9476	There is no RESTful API command to get/list the installed custom rule data files.
PD-9507	Unable to add an SDN controller using the RESTful API/WUI in a specific scenario.
PD-9553	There is no API command to disable secure NTP mode.
PD-9816	There is an API command to list individual rules in a ruleset, but there is no command to list the available rulesets themselves.
PD-9947	Virtual Services/Real Servers can report as "Up" in the API even if SubVSs are disabled.
PD-10363	The PowerShell API is missing the **ServerFbaPath** and **ServerFBAPost** parameters.
PD-10421	Setting options for the syslog server settings multiple times for different levels using the API causes events to repeat.
PD-10490	The **vsremovewafrule** RESTful API command does not allow multiple rules to be removed.
PD-10577	Some API calls are failing due to NULL pointers.
PD-10598	There is no PowerShell API parameter to modify the **IdP Certificate Match** option.

4 Release 7.2.40.1

The following issues have been resolved in this hotfix release. If you require this LoadMaster firmware version please contact KEMP Customer Support at https://support.kemptechnologies.com/hc/en-us/requests/new

Refer to the sections below for details about firmware version 7.2.40.1.

4.1 7.2.40.1 - Issues Resolved

PD-10392	Improved LoadMaster stability when upgrading from firmware version 7.2.39 to 7.2.40.1.
PD-10367	Previously, a race condition on a connection close (local) and reset (peer) may have caused the system to become unstable. Now, protective error handling mitigates this behavior.
PD-10258	Previously, HTTP Strict Transport Security (HSTS) headers were added by default during processing of responses which caused issues with some non-SSL services. Now, the behavior is configurable within the Virtual Service **SSL Properties**.
PD-10249	Previously, non-XML/JSON payloads were not passed through the Web Application Firewall (WAF) engine for inspection, therefore avoiding potential detection of malicious content. Now, all content type payloads can be inspected based on WAF configuration options.
PD-10191	Previously, IPsec connections were failing to establish due to a change in cryptography requirements. Now, connections can be established because the LoadMaster was updated to support the required cryptography.
PD-10177	Previously, the HTTP/2 stack in certain web apps mishandled cookies causing inconsistent behavior in different browsers. Now, the cookie behavior is normalized for all browsers.
PD-10114	Previously, the Edge Security Pack (ESP) user logs did not contain User Agent information. Now, User Agent information can be included by enabling the **Include User Agent Header in User Logs** check box in the **L7 Configuration** screen.

4.2 7.2.40.1 - Known Issues

PD-10980	A critical vulnerability in the LoadMaster Operating System (LMOS) related to Session Management could allow an unauthorized, remote attacker to bypass security protections, gain system privileges, and execute elevated commands such as **ls**, **ps**, **cat**, and so on, thereby compromising the system. Through this remote execution, in certain

	cases, exposure of sensitive system data such as certificates, private keys, and other information may be possible. Further information can be found here: Mitigation For Remote Access Execution Vulnerability.
PD-8725	Proximity and Location Based scheduling does not work with IPv6 source addresses.
PD-9765	GEO does not support DNS TCP requests from unknown sources.
PD-10155	Issue with configuration corruption causes some GEO features not to function.
PD-10374	User credentials are shown in LDAP Endpoint health check Wireshark captures.
PD-10355	There are some authentication issues with SAML when opening a second tab before authenticating.
PD-10245	Extended logs can only be selected by date.
PD-10239	The IPsec Pre Shared Key (PSK) is stored in plain text in backups.
PD-10235	The Adaptive Agent log file is causing the disk to become full when the SDN Adaptive add-on is not enabled.
PD-10207	The ESP logs need to be made more accurate.
PD-10205	The ESP Form Authentication Path does not support underscores or dashes.
PD-10197	The status of cluster Virtual Services and Real Servers are reported incorrectly on the home page.
PD-9944	There is an incorrect character limitation on Header Modification Rules.
PD-10409	WAF does not block attack requests if the POST request does not contain the "content-type" header.
PD-10141	Service check interval configuration causes dropped connections.
PD-10193	A WAF, ESP, and KCD configuration with Microsoft Exchange 2010 is not supported.
PD-10126	Issues with cache causes connection problems.
PD-10086	When selecting the 'Use for Default Gateway' option on a new interface, access to the LoadMaster WUI is lost. However, there is still access to the LoadMaster using the local IP address.
PD-10083	There is an issue displaying a large number of Virtual Services/SubVSs when using SNMP.
PD-10080	Failover issues occur with bonded interfaces that are configured to use the default gateway.

PD-10042	WAF statistics do not get reset on Virtual Service deletion.
PD-10040	WAF does not support chunked transfer encoding on the POST body.
PD-10039	The HTTP/2 feature is only supported in the Internet Explorer (IE) browser.
PD-9975	When testing LDAP-based users by using the **Test AAA for User** on the **WUI Authentication and Authorization** page, logs were not generated or visible in syslog.
PD-9764	The LoadMaster is unable to set up an IPsec tunnel to Azure classic/Azure Resource Manager (ARM) endpoints.
PD-8697	Some users are having issues detecting the partition when using the Hardware Security Module (HSM).
PD-10188	When adding a Real Server to a Virtual Service or SubVS on a Safari browser, the list of available Real Servers is not available.
PD-10131	Problems attaching files in SharePoint when using WAF with process response enabled and Kerberos Constrained Delegation (KCD).
PD-10159	When upgrading firmware from 7.1.35.*x*, CPU and network usage graphs are not appearing. As a workaround, reset the statistics in the WUI.
PD-10143	Access is denied when KCD, the WAF **Process Responses** option and the **creditcard_track_pan** rule are enabled.
PD-9375	Microsoft Office files in SharePoint do not work in Firefox and Chrome when using SAML authentication.
PD-10095	When L7 debugging is enabled, Virtual LoadMasters may reboot in certain situations.
PD-7156	The **VSIndex** parameter is missing in some API commands.
PD-9476	There is no RESTful API command to get/list the installed custom rule data files.
PD-9525	The RESTful API returns the value of the **failtime** parameter in seconds, but it is set in minutes.
PD-9539	There are issues with the PowerShell **New-GeoCluster** command in a specific scenario.
PD-9553	There is no API command to disable secure NTP mode.
PD-9570	There is a typo in the **removecountry** API response error message.
PD-9572	There are discrepancies displaying the location latitude/longitude parameter values for some RESTful API commands.

5 Release 7.2.40

Refer to the sections below for details about firmware version 7.2.40. This was released on 1st November 2017.

5.1 7.2.40 - New Features

The following features were added to the 7.2.40 release:

- Activation Server Local (ASL) LoadMasters have the ability to download Web Application Firewall (WAF) commercial rules and GEO IP blacklist rules.
- A LoadMaster Web User Interface (WUI) Help menu option to provide knowledge about External Services provided by KEMP.

5.2 7.2.40 - Feature Enhancements

- The Call Home feature is now an opt-out process during initial activation of a LoadMaster.
- Added support in the LoadMaster for the following OWASP secure HTTP response headers: X-Frame-Options, X-XSS-Protection, X-Content-Type-Options, HSTS Strict-Transport-Security.
- Added the ability to easily delete a Virtual Service and all its nested SubVSs.
- Real Server enhancements:

  - Added the ability to select from the available list of Real Servers when configuring a Virtual Service or SubVS.

  - On the **Real Servers** screen, it is possible to sort the Real Server addresses or the status column by clicking the column label.

  - When adding a Real Server to a SubVS, a check box appears that enables you to assign that Real Server to all other SubVSs of the main Virtual Services.
- Added the ability to use the DNS name as the Online Certificate Status Protocol (OCSP) server.
- In SAML authentication, the URL provided in the original request from Layer 7 is preserved. This URL gets precedence over the destination URL from the SAML response.
- Improvements to using FQDN to designate to a Real Server; there is now a configurable **DNS Update Interval**. Also, **Reload DNS Entries for Real Server Errors** can be enabled to allow a reload of DNS entries when health checks have errors and an FQDN is associated with the Real Server IP address.
- When an OCSP server fails to connect, error logs are printed.

5.3 7.2.40 - Issues Resolved

PD-9886	Fixed a security issue with the initial boot password in the Azure Virtual LoadMaster logs.
PD-9838	Fixed a security issue where the full session ID was printed in the logs. Now, only a partial session ID is printed.
PD-9837	Fixed an issue with the WUI admin login in **Password or Client certificate mode**.
PD-9768	Fixed a security issue when the 'Logon Transcode' option and ESP are enabled.
PD-9892	Fixed an issue preventing SNORT rules from being applied.
PD-9889	Transparency is removed if the connection to the Real Server is part of a HTTP/2 connection.
PD-9972	Edge Security Pack (ESP) group Common Name and Domain Name can be up to 127 characters long.
PD-9898	Fixed an issue with configuration corruption that caused some GEO features to not function.
PD-9865	Fixed issues that prevented automatic update of GEO IP blacklist rules.
PD-9861	An ESP re-authentication is forced when a closed session is reopened after a user terminates without logging out.
PD-9795	Fixed an issue that caused SAML response decoding to fail.
PD-9770	Added more information to the ESP logs.
PD-9761	Made enhancements to support a high number of connections.
PD-9743	Fixed an issue relating to exporting a template for a Virtual Service that has content switching enabled with default rules.
PD-9666	Fixed an issue with underscores in HTTP header name which is not handled by Apache server 2.4.
PD-9633	Fixed an issue when using HTTP/1.1 to enable the port number to be used with Checkhost.
PD-9517	Applied username normalization when permitted groups are configured to permit authentication.
PD-9508	With ESP and SAML, the certificate in the SAML response must match the certificate assigned in the SAML SSO domain. This limits the solution to trusted certificates.

PD-9470	Fixed an issue with LDAP Real Server health checks.
PD-9453	Removed pinging of default gateway and nameserver in Azure because they are not supposed to work.
PD-9359	Fixed an issue causing problems for some users authenticating to ESP.
PD-9159	Fixed an issue causing traffic to the back-end to be blocked in certain scenarios when the Web Application Firewall (WAF) is enabled.
PD-10107	Fixed an issue that caused WAF to be inactive upon first licensing in certain scenarios.
PD-10089	Fixed an issue that caused WAF **Process Responses** to be inactive in certain situations.
PD-10062	Improved error handling when there is an invalid FQDN in OCSP configuration.
PD-9995	Fixed a client certificate issue preventing users from accessing SharePoint or OWA.
PD-9908	Fixed an issue with ESP steering groups.
PD-9903	Fixed an issue with multiple Network Interface Cards (NICs) on Azure Virtual LoadMasters and private IP addresses.
PD-9869	Fixed an issue in Content Rules that caused a rule to be deleted if a 'white space' was the only thing in the 'replacement text' field.
PD-9867	Fixed an issue preventing the global connection timeout from being honored on Virtual Services.
PD-9857	Fixed a rare situation that caused HTTP/2 to crash when using 'RS drop on fail'.
PD-9845	Improved compatibility for Arabic characters when generating local certificates.
PD-9783	Fixed an issue causing the incorrect IP address to be displayed in the tool-tip text on High Availability (HA) icons.
PD-9758	Fixed an issue preventing customers from editing or accessing Office files in SharePoint.
PD-9747	Fixed an issue preventing HA from working with certificate authentication and KEMP 360.
PD-9604	Fixed an import issue preventing Content Rules from being correctly applied to a SubVS.
PD-9590	Improved the subscription expiry display date to be more accurate.
PD-9657	The LoadMaster handles cipher names with special characters better.
PD-9643	Fixed an issue in Azure to permit mapping of IP addresses and add the ability to

	change IP addresses if a match is not found.
PD-9560	Improved error handling when clicking the shared IP address in HA mode.
PD-9383	Improved error handling for special characters in passwords when working with KEMP 360.
PD-8227	Fixed an issue preventing the addition of network/addresses in the GEO IP blacklist.
PD-7157	Fixed an issue preventing users from attaching files when using OWA or SharePoint if WAF and Kerberos Constrained Delegation (KCD) are both enabled.
PD-8413	Fixed an issue that caused an error if a wildcard port was in a template.
PD-9489	Fixed an issue with the Application Program Interface (API) command to reset the CPU and network usage.
PD-9963	Fixes made to the PowerShell API wrapper in relation to Activation Server Local (ASL) functionality and its interaction with KEMP 360.
PD-9883	Improved error handling when creating Virtual Services with specific ports using the API.
PD-9836	Improved compatibility in the RESTful API when using a Polish character set in passwords.
PD-9781	Added missing parameters to the **New-AdcContentRule** and **Set-AdcContentRule** commands in the PowerShell API.
PD-9779	Made the WUI and RESTful API consistent for the Client Authentication Mode ESP parameter.
PD-9771	Fixed a situation that caused the RESTful API to report the wrong status for disabled/down Virtual Services.
PD-9596	Fixed an issue causing the RESTful API to show an incorrect interface value in the **showiface** command output.
PD-9360	Fixed an issue that caused a crash when restoring a LoadMaster backup with 'Type' All, Base, Base+VS and Base+Geo using the RESTful API.
PD-9349	Fixed the PowerShell API wrapper command **Get-AslLicenseType** in relation to new ASL behavior.
PD-7978	Fixed an issue with the PowerShell API command **New-TlsHSMClientCert**that caused an error when the **LoadBalancer** and **Credential/SubjectCN** parameters were used.
PD-9129	Fixed an issue with the response formatting in the API backup commands.

5.4 7.2.40 - Known Issues

PD-10980	A critical vulnerability in the LoadMaster Operating System (LMOS) related to Session Management could allow an unauthorized, remote attacker to bypass security protections, gain system privileges, and execute elevated commands such as **ls**, **ps**, **cat**, and so on, thereby compromising the system. Through this remote execution, in certain cases, exposure of sensitive system data such as certificates, private keys, and other information may be possible. Further information can be found here: Mitigation For Remote Access Execution Vulnerability.
PD-8725	Proximity and Location Based scheduling does not work with IPv6 source addresses.
PD-9765	GEO does not support DNS TCP requests from unknown sources.
PD-10155	Issue with configuration corruption causes some GEO features not to function.
PD-10392	Random reboots can occur on the master unit after upgrading the firmware to 7.2.39 and patching to 7.2.39.1 or 7.2.40.
PD-10141	Service check interval configuration causes dropped connections.
PD-10193	A WAF, ESP, and KCD configuration with Microsoft Exchange 2010 is not supported.
PD-10126	Issues with cache causes connection problems.
PD-10086	When selecting the 'Use for Default Gateway' option on a new interface, access to the LoadMaster WUI is lost. However, there is still access to the LoadMaster using the local IP address.
PD-10083	There is an issue displaying a large number of Virtual Services/SubVSs when using SNMP.
PD-10080	Failover issues occur with bonded interfaces that are configured to use the default gateway.
PD-10042	WAF statistics do not get reset on Virtual Service deletion.
PD-10040	WAF does not support chunked transfer encoding on the POST body.
PD-10039	The HTTP/2 feature is only supported in the Internet Explorer (IE) browser.
PD-9975	When testing LDAP-based users by using the **Test AAA for User** on the **WUI Authentication and Authorization** page, logs were not generated or visible in syslog.
PD-9764	The LoadMaster is unable to set up an IPsec tunnel to Azure classic/Azure Resource Manager (ARM) endpoints.
PD-8697	Some users are having issues detecting the partition when using the Hardware Security

	Module (HSM).
PD-10188	When adding a Real Server to a Virtual Service or SubVS on a Safari browser, the list of available Real Servers is not available.
PD-10131	Problems attaching files in SharePoint when using WAF with process response enabled and Kerberos Constrained Delegation (KCD).
PD-10159	When upgrading firmware from 7.1.35.*x*, CPU and network usage graphs are not appearing. As a workaround, reset the statistics in the WUI.
PD-10143	Access is denied when KCD, the WAF **Process Responses** option and the **creditcard_track_pan** rule are enabled.
PD-9375	Microsoft Office files in SharePoint do not work in Firefox and Chrome when using SAML authentication.
PD-10095	When L7 debugging is enabled, Virtual LoadMasters may reboot in certain situations.
PD-7156	The **VSIndex** parameter is missing in some API commands.
PD-9476	There is no RESTful API command to get/list the installed custom rule data files.
PD-9525	The RESTful API returns the value of the **failtime** parameter in seconds, but it is set in minutes.
PD-9539	There are issues with the PowerShell **New-GeoCluster** command in a specific scenario.
PD-9553	There is no API command to disable secure NTP mode.
PD-9570	There is a typo in the **removecountry** API response error message.
PD-9572	There are discrepancies displaying the location latitude/longitude parameter values for some RESTful API commands.

6 Release 7.2.39.1

Refer to the sections below for details about firmware version 7.2.39.1. This was released on 6th September 2017.

6.1 7.2.39.1 - Feature Enhancements

- Support for LoadMaster Service Provider License Agreements (SPLA) added to Amazon Web Services (AWS).
- Additional enhancements made to the Edge Security Pack (ESP) connection logs.

6.2 7.2.39.1 - Issues Resolved

PD-9872	Fixed an issue where the Web Application Firewall (WAF) was not blocking specific requests when rules were enabled to do so.
PD-9879	Fixed an issue that caused a delay with UDP connections.
PD-9844	Fixed an issue that was causing LoadMaster reboots.

6.3 7.2.39.1 - Known Issues

PD-10980	A critical vulnerability in the LoadMaster Operating System (LMOS) related to Session Management could allow an unauthorized, remote attacker to bypass security protections, gain system privileges, and execute elevated commands such as **ls**, **ps**, **cat**, and so on, thereby compromising the system. Through this remote execution, in certain cases, exposure of sensitive system data such as certificates, private keys, and other information may be possible. Further information can be found here: Mitigation For Remote Access Execution Vulnerability.
PD-8725	Proximity and Location Based scheduling does not work with IPv6 source addresses.
PD-9765	GEO does not support DNS TCP requests from unknown sources.
PD-10392	Random reboots can occur on the master unit after upgrading the firmware to 7.2.39 and patching to 7.2.39.1.
PD-9892	**Application of SNORT rules does not work.**
PD-10155	Issue with configuration corruption causes some GEO features not to function.
PD-9886	Password defined at deployment on Azure cloud appears in log. **Note:** KEMP strongly recommend that the password set at deployment in Azure is

	changed to mitigate this issue.
PD-9657	Naming a cipher set using **-** or **+** results in some issues.
PD-9908	ESP steering groups are not working as expected.
PD-9903	Adding additional private IP addresses to Azure LoadMasters only works if there is more than one Network Interface Card (NIC).
PD-9898	GEO IP range selection queries are refused in certain scenarios.
PD-9869	Adding a space in the **Replacement text** field of an existing body replacement rule deletes the rule.
PD-9867	There are some issues with the global connection timeout default value.
PD-9865	There are some issues with the GEO IP blacklist automatic updates.
PD-9861	There are some security issues with Outlook Web Access (OWA) when using ESP.
PD-9857	Using **RS drop on fail** with HTTP/2 connections may cause the kernel to panic.
PD-9837	WUI admin password login does not work in **Password or Client certificate** mode (except for the **bal** user).
PD-9795	Decoding is failing for some base64 certificates when using Security Assertion Markup Language (SAML) authentication.
PD-9770	ESP logs missing some information.
PD-9768	Security issue in the SSO debug logs relating to the logon transcode option.
PD-9761	There are some issues dealing with a high number of connections.
PD-9758	Some users are unable to edit or access Office files from SharePoint when using SAML and KCD authentication.
PD-9747	Some issues using HA pairs with certificate authentication.
PD-9743	Issues importing some template files that have the default rule assigned.
PD-9666	Headers with underscores are not accepted by Apache 2.4.
PD-9643	Unable to change the IP address of a Virtual Service in an Azure LoadMaster.
PD-9633	Unable to set the check host with the port attached in the WUI (it works using the API or CLI).
PD-9604	Issues when trying to import some custom templates.
PD-9517	Unable to authenticate some users when the password is expired and permitted groups

	are used.
PD-9508	ESP only verifies SAML assertions when using the root certificate.
PD-9504	Some users are experiencing issues with HA failover on Multi-Tenant LoadMaster units.
PD-10159	CPU and network usage graphs not appearing after firmware upgrade. Resetting the statistic counters does not clear the graph data.
PD-9453	Some Azure users are having issues licensing due to communication issues with the default gateway.
PD-9383	Some issues with special space characters for local LoadMaster user authentication.
PD-9359	Some users unable to authenticate using ESP.
PD-9159	When WAF is enabled there is no traffic on the back-end in certain scenarios.
PD-8697	Some users having issues detecting the partition when using the Hardware Security Module (HSM).
PD-7157	When using WAF and KCD, all file attachments in SharePoint fail.
PD-9470	LDAP Real Server health checking is not working optimally.
PD-9883	The **addvs** API command incorrectly allows a Virtual Service to be created on the same IP address and port as the LoadMaster Web User Interface (WUI).
PD-9864	The API on the Multi-Tenant LoadMaster is not working when **Require Basic Authentication** is enabled in **WUI Session Management**.
PD-9779	Discrepancies between the WUI and RESTful API parameter for "Client Authentication Mode".
PD-9596	The showiface RESTful API command shows the wrong interface values in the output for interfaces that are not configured.
PD-9572	There are discrepancies displaying the location latitude/longitude parameter vales for some RESTful API commands.
PD-9570	There is a typo in the removecountry API response error message.
PD-9553	There is no API command to disable secure NTP mode.
PD-9539	Issues with the PowerShell New-GeoCluster command in a specific scenario.
PD-9525	The RESTful API returns the value of the failtime parameter in seconds, but it is set in minutes.
PD-9523	In a specific scenario, the RESTful API returns a success message when fetching a non-

	existing GEO FQDN.
PD-9476	There is no RESTful API command to get/list the installed custom rule data files.
PD-9129	The API command to backup contains an error that breaks the PowerShell wrapper connection.
PD-7156	The **VSIndex** parameter is missing in some API calls.
PD-10160	The API commands to reset the CPU and network graphs do not work.

7 Release 7.2.39

Refer to the sections below for details about firmware version 7.2.39. This was released on 2nd August 2017.

7.1 7.2.39 - New Features

The following features were added to the 7.2.39 release:

- Response body modification rules
- Added HTTP/2 support
- Azure Marketplace Syndication for LoadMaster supported on Azure Stack TP3
- Published the following Virtual Service application configuration templates:
  - Aequitas
  - Cerner Health
  - eClinicalWorks
  - Horizon Flex
  - Seclore
  - NextCloud
- Enhanced cloud High Availability (HA)

7.2 7.2.39 - Feature Enhancements

- Updated OpenSSH to version 7.5.p1.
- Enhanced the Edge Security Pack (ESP) connection logs.
- Added form-based to form-based authentication support for Microsoft Exchange 2010.
- Added an option to selectively restore ESP Single Sign On (SSO) configuration settings.
- Updated the PowerShell module to reflect Microsoft standards.

  This PowerShell module is not backwards compatible with previous PowerShell modules from KEMP Technologies.

- Optimized Web Application Firewall (WAF) logging for disk storage.

7.3 7.2.39 - Issues Resolved

PD-9627	Stopped cookie values displaying in the Web User Interface (WUI).
PD-9588	It is possible to modify the IP address of the shared IP on a VLAN interface.
PD-9556	Fixed an issue with GEO custom locations.
PD-9551	It is possible to have GEO FQDN names containing underscores.
PD-9549	Fixed an issue which prevented some users from accessing some Virtual Services when using WAF.
PD-9522	Fixed an issue that caused content rules to disappear when SSL re-encryption was enabled.
PD-9492	Fixed an issue that was causing LM-5600 models to lose configuration after a reboot.
PD-9457	Fixed an issue that caused an error relating to sending and receiving completion packets.
PD-9456	Fixed automated backup processing for the SCP method to allow underscores in usernames.
PD-9450	Fixed an issue that was causing OCSP to not permit valid users in certain scenarios.
PD-9402	Fixed an issue that was causing users to disconnect when using RSA authentication and logging into different applications with different browsers.
PD-9401	Fixed an issue with the **Drop Connections on RS failure** that caused high RAM usage.
PD-9393	Fixed a memory issue with the SSO manager.
PD-9389	Fixed an issue that prevented Layer7 from initializing when processing SNORT rules.
PD-9362	Fixed an issue that caused Real Servers to be forced in a disabled state globally, even if it was enabled on all Virtual Services.
PD-9335	Fixed an issue that prevented server-side SSO domains from being deleted.
PD-9290	Removed "deprecated option" SSO manager logs.
PD-9258	Fixed an issue that prevented some users from accessing the LoadMaster after upgrading the firmware.
PD-9253	Removed unnecessary logs relating to WAF in the passive unit.
PD-9239	Fixed an issue that caused the LoadMaster to reboot when the persistence mode of a UDP syslog Virtual Service was changed.
PD-9236	Fixed an issue that was causing HA MELA (Metered Enterprise License Agreement) LoadMasters to have network failure every five minutes.
PD-9229	Fixed an issue that was causing units to reboot and go into a pacified state after upgrading

	the firmware.
PD-9218	Fixed an issue that was preventing users from signing into the WUI using LDAP credentials.
PD-9206	Improved special character handling for forms-based server-side passwords.
PD-9183	Fixed an issue that was causing a segfault in certain situations.
PD-9160	Fixed an issue that was causing WAF to block the uploading of files larger than 1MB.
PD-9158	Fixed an issue that caused SNMP traps to come from individual IPs and not from the Shared IP, even when the **Send SNMP traps from the shared address option** was enabled.
PD-9154	Fixed an issue with the OWA expired password functionality in Exchange 2010.
PD-9136	Fixed an issue with subnet originating when doing re-encryption in cluster mode.
PD-9133	Fixed the log level for some licensing response information.
PD-9123	Fixed an issue that was preventing the default content rule from being selected.
PD-9121	Fixed an issue with client certificate authentication.
PD-9114	Fixed an issue that was causing email alerts to not work if the hostname contained an underscore.
PD-9112	Fixed an issue that was preventing the IP address of the SubVS from being shown in the WAF real time statistics.
PD-9107	Fixed an issue that was preventing authentication using LDAP.
PD-9074	Improved error message relating to destination IP addresses and ESP session management.
PD-9062	Fixed an issue that caused simultaneous health check failures.
PD-9059	Improved GEO error handling.
PD-9045	Fixed an issue that caused email logging to not use the current hostname as the **MAIL FROM**.
PD-9041	Fixed an issue with WAF that caused a specific web feature to fail.
PD-9039	Fixed an issue that caused WAF to break a Virtual Service when a HA pair failed over twice.
PD-8986	Fixed an issue that caused a slow download speed in certain situations.
PD-8915	Fixed an issue with Hyper-V live migration.
PD-8896	Fixed an issue that was preventing some customers from editing or accessing Office files from SharePoint when using SAML authantication.
PD-8558	Fixed an issue that caused Outlook clients to connect slowly through a Virtual Service when set up with a template.

PD-8320	Fixed an issue that prevented SDN from connecting to the HP SDN controller.
PD-9384	Fixed a typo in the Enable Session Management check box hover text.
PD-9356	Syslog entries are no longer duplicated.
PD-9181	Fixed an issue that partially exposed the SCP automated backup key.
PD-9174	Fixed an issue that prevented backing up using FTP using the console.
PD-8953	Fixed a spelling error in the WUI in the **Allow Administrative WUI Access** check box label.
PD-7265	Users are now redirected to the new shared IP address when it is changed.
PD-9285	Fixed the response code when setting the **wuildapep** parameter with an invalid LDAP EP.
PD-9153	Fixed an issue that stopped a SubV-generated WAF event from being accepted by mlogc.
PD-9151	The **Reset Statistic Counters** option now resets WAF stats.
PD-9060	Fixed an issue that caused some mlogc instances taking 100% CPU usage after WAF remote logging was disabled.
PD-8969	Fixed an issue that prevented WAF automated installations from working on initial setup.
PD-8968	Changing the HA shared IP address on a KVM-based LoadMaster happens instantly (without rebooting).
PD-8750	Fixed an issue that was causing WUI access to fail if the multi-interface access was changed.
PD-9624	Mitigated against the CVE-2017-8890 vulnerability.
PD-9355	Fixed an issue with authentication using client certificates in certain scenarios.
PD-9096	Daily, zipped ESP extended log files are automatically generated.
PD-8958	SSO sessions now display sessions when client SAML SSO users login to OWA.
PD-8413	It is possible to specify a wildcard port when creating Virtual Services using a template.
PD-8196	Improved error handling for RESTful API command **enablewafremotelogging**.
PD-8118	Added a parameter to get the GEO update interface using the API.
PD-8107	Added an option to force an NTP update using the API.
PD-7613	Improved the **showiface** API command to show more parameters.
PD-9176	Improved the EULA API output for Azure.
PD-9099	Fixed an issue with the **delintermediate** API command.

PD-8727	It is possible to delete the IP range using the API (even if it includes IPv6).
PD-9593	Fixed an issue that was preventing connectivity to the base IP address when configuring the shared IP address for HA using the RESTful API.
PD-9581	Fixed an issue with the output of the PowerShell **Set-GeoMiscParameter** command.
PD-9439	Fixed an issue with the output of the **Set-LmHAMode** command.
PD-9378	Improved error when using the RESTful API to add a white/black list address to an unknown Virtual Service.
PD-9132	Restoring a configuration using the API works.
PD-9346	Fixed an issue with the **Uninstall-LmPatch** PowerShell command.
PD-9343	Improved error when deleting a non-existing LoadMaster add-on using the RESTful API.
PD-9260	It is possible to change the password of a local user using the RESTful API.
PD-9255	Improved error handling for the RESTful API command **uploadsamlidpmd**.
PD-9148	It is possible to unset the email server port and syslog server port using the RESTful API.
PD-9108	Improved error handling when deleting non-existing routes using the RESTful API.

7.4 7.2.39 - Known Issues

PD-10980	A critical vulnerability in the LoadMaster Operating System (LMOS) related to Session Management could allow an unauthorized, remote attacker to bypass security protections, gain system privileges, and execute elevated commands such as **ls**, **ps**, **cat**, and so on, thereby compromising the system. Through this remote execution, in certain cases, exposure of sensitive system data such as certificates, private keys, and other information may be possible. Further information can be found here: Mitigation For Remote Access Execution Vulnerability.
PD-8725	Proximity and Location Based scheduling does not work with IPv6 source addresses.
PD-9765	GEO does not support DNS TCP requests from unknown sources.
PD-10392	Random reboots can occur on the master unit after upgrading the firmware to 7.2.39.
PD-9821	Some high memory usage has been observed in firmware version 7.2.39.
PD-9892	**Application of SNORT rules does not work.**

PD-10155	Issue with configuration corruption causes some GEO features not to function.
PD-9844	An issue is causing LoadMaster reboots.
PD-9877	There is a minor delay in UDP Virtual Services.
PD-9793	WAF does not block attack traffic or requests even though the appropriate rule is assigned in the Virtual Service. To resolve this problem, enable the **Inspect HTML POST Request Content** check box.
PD-9758	Some users are unable to edit or access Office files from SharePoint when using SAML and KCD authentication.
PD-9770	ESP logs missing some information.
PD-9159	When WAF is enabled there is no traffic on the back-end in certain scenarios.
PD-9666	Headers with underscores are not accepted by Apache 2.4.
PD-9633	Unable to set the check host with the port attached in the WUI (it works using the API or CLI).
PD-9517	Unable to authenticate some users when the password is expired and permitted groups are used.
PD-9508	ESP only verifies SAML assertions when using the root certificate.
PD-9504	Some users are experiencing issues with HA failover on Multi-Tenant LoadMaster units.
PD-10159	CPU and network usage graphs not appearing after firmware upgrade. Resetting the statistic counters does not clear the graph data.
PD-9470	LDAP Real Server health checking is not working optimally.
PD-9453	Some Azure users are having issues licensing due to communication issues with the default gateway.
PD-9359	Some users unable to authenticate using ESP.
PD-8697	Some users having issues detecting the partition when using the Hardware Security Module (HSM).
PD-9768	Security issue in the SSO debug logs relating to the logon transcode option.
PD-9657	Naming a cipher set using **-** or **+** results in some issues.
PD-9643	Unable to change the IP address of a Virtual Service in an Azure LoadMaster.
PD-9604	Issues when trying to import some custom templates.

PD-9747	Some issues using HA pairs with certificate authentication.
PD-9383	Some issues with special space characters for local LoadMaster user authentication.
PD-7157	When using WAF and KCD, all file attachments in SharePoint fail.
PD-7156	The **VSIndex** parameter is missing in some API calls.
PD-9575	There are issues with some **aclcontrol** API commands.
PD-9129	The API command to backup contains an error that breaks the PowerShell wrapper connection.
PD-9596	The **showiface** RESTful API command shows the wrong interface values in the output for interfaces that are not configured.
PD-9572	There are discrepancies displaying the location latitude/longitude parameter vales for some RESTful API commands.
PD-9570	There is a typo in the **removecountry** API response error message.
PD-9553	There is no API command to disable secure NTP mode.
PD-9539	Issues with the PowerShell **New-GeoCluster** command in a specific scenario.
PD-9525	The RESTful API returns the value of the **failtime** parameter in seconds, but it is set in minutes.
PD-9523	In a specific scenario, the RESTful API returns a success message when fetching a non-existing GEO FQDN.
PD-9476	There is no RESTful API command to get/list the installed custom rule data files.
PD-7978	The **New-TlsHSMClientCert** command returns an error when the **LoadBalancer** and **Credential/SubjectCN** parameters are used.
PD-10160	The API commands to reset the CPU and network graphs do not work.

8 Release 7.2.38

Refer to the sections below for details about firmware version 7.2.38. This was released on 3rd April 2017.

8.1 New Features

The following features were added to the 7.2.38 release:

- Introduced a tiered subscription licensing model.
- The following Virtual Service application configuration templates were published:
  - Zimbra
  - Deepnet DualShield
  - Luminis (Banner)

8.2 Feature Enhancements

- Updated the OpenSSH version to 7.4p1.
- Updated the OpenSSL version to 1.0.2k to mitigate against the following vulnerabilities:
  - CVE-2017-3731
  - CVE-2017-3730
  - CVE-2017-3732
  - CVE-2016-7055
- The LoadMaster passes more configuration information back to KEMP.
- Support added for OWASP CRS 3.0 rules.
- Improved the hover text for High Availability (HA) status indicators.
- Automated backups can use SCP and FTP.
- Improved debugging API command XML output.

8.3 Issues Resolved

PD-8602	Logs display both the Fully Qualified Domain Name (FQDN) and IP address for Real Server messages when the FQDN is used as the Real Server.
PD-8477	Improved the icon used to indicate the default Real Server when using fixed

	weighting.
PD-8985	Fixed an issue with creating custom cipher sets.
PD-8983	Fixed an issue that stopped ActiveSync from working.
PD-8966	Fixed an issue with remote syslog ports.
PD-8947	Fixed an issue that was preventing compression from working with HTTP Virtual Services.
PD-8890	Fixed an issue with the Edge Security Pack (ESP) Username field.
PD-8846	Fixed a GEO issue that was giving private answers to public clients.
PD-8771	Fixed a SAML issue that was directing users to the IdP SSO URL instead of the IdP Logoff URL when logging off.
PD-8760	The LoadMaster no longer displays an incorrect message saying the Web Application Firewall (WAF) rulesets are out-of-date when, in some cases, they are not.
PD-8730	Fixed an issue preventing clients from authenticating using ESP, in some cases.
PD-8657	Fixed an issue preventing some files hosted by PowerSchool from downloading.
PD-8642	Stopped an incorrect error log being generated when an automated backup is successful.
PD-8636	Fixed an issue that showed FQDNs as enabled even if it was disabled globally.
PD-8581	Fixed an issue preventing filtered ESP logs from displaying.
PD-8568	Stopped an unnecessary error message from being displayed when viewing log files.
PD-8953	Fixed a typo in the Remote Access screen in the Web User Interface (WUI).
PD-8869	An error message appears when adding an extra port that conflicts with another Virtual Service.
PD-9031	Stopped unnecessary errors from appearing in the LoadMaster console screen.
PD-8972	Fixed a WUI issue that was not displaying the RADIUS Server(s) or RADIUS Shared Secret fields values.
PD-8772	Fixed an issue that was obstructing the serial number field in the LoadMaster

	console.
PD-8965	You can enable/disable TCP Multiple Connect even when the license does not have Multiple Connect.
PD-8014	Remote GEO LoadMasters are marked as up, even if they contain no Virtual Service addresses.
PD-8766	"Everywhere" only appears once in the GEO location selection.
PD-8713	Fixed an issue that was preventing some content rules from matching in certain scenarios.
PD-8882	Fixed an issue that was preventing the Real Server destination port from being set using the Application Program Interface (API).
PD-8654	Fixed an issue preventing the Use HTTP/1.1 setting from being configured using the API.
PD-8716	Improved the output of the showdomainlockedusers API command.
PD-8545	Fixed an issue with the Initialize-LoadBalancer PowerShell API command.
PD-8848	Improved error handling for the Request-KEMPLicenseOffline and Update-KEMPLicenseOffline PowerShell API commands.
PD-8988	Fixed an issue that was causing kernel panic in some scenarios.
PD-8649	Fixed an issue that prevented firmware patches from being applied when /tmp is partially full (~17%).
PD-8746	Fixed issues with downloading/installing WAF rules after doing a factory reset.
PD-8378	Improved error handling with the **listvs** API command.
PD-8561	Improved the response for the **createbond** and **unbond** API commands.
PD-8357	Fixed an issue with error handling when adding a new cluster using the API.
PD-8992	Improved email logging.
PD-8656	Fixed an issue with the **aslactivate** API command.
PD-8731	Fixed an issue with the GEO blacklist functionality.
PD-8857	Improved output of the **Get-LicenseType** command.
PD-8411	Fixed an issue with importing the PowerShell module file.

8.4 Known Issues

PD-10980	A critical vulnerability in the LoadMaster Operating System (LMOS) related to Session Management could allow an unauthorized, remote attacker to bypass security protections, gain system privileges, and execute elevated commands such as **ls**, **ps**, **cat**, and so on, thereby compromising the system. Through this remote execution, in certain cases, exposure of sensitive system data such as certificates, private keys, and other information may be possible. Further information can be found here: Mitigation For Remote Access Execution Vulnerability.
PD-9892	**Application of SNORT rules does not work.**
PD-10155	Issue with configuration corruption causes some GEO features not to function.
PD-7265	When you change the Shared IP Address in a HA pair, you are not redirected to the new Shared IP Address.
PD-8413	Cannot specify wildcard port when creating a Virtual Service from a template.
PD-8725	Proximity and Location Based scheduling does not work with IPv6 source addresses.
PD-8561	No response received when running the createbond/unbond API commands, even when they are successful.
PD-8196	When using the enablewafremotelogging API command it is possible to set the remote URI to an invalid format.
PD-8118	The GEO Update Interface cannot be set using the API.
PD-8107	It is not possible to force an NTP update using the API.
PD-7613	The showiface and modiface API commands do not show the User for Cluster Checks and Use for Cluster Updates options.
PD-7156	The VS index parameter is missing from some API commands.
PD-9070	Check Interval not displaying correct value when using API
PD-9059	GEO Error Messages
PD-8881	Powershell Get-Virtualservice: the cmdlet does not return a valid PS object
PD-7265	No redirection when Shared IP is changed using the WUI
PD-10160	The API commands to reset the CPU and network graphs do not work.

9 Release 7.2.37.1

Refer to the sections below for details about firmware version 7.2.37.1. This was released on 7th February 2017.

9.1 New Features

The following features were added to the 7.2.37.1 release:

- Security Assertion Markup Language (SAML) support added.
- Edge Security Pack (ESP) form-based to form-based authentication.
- Hardware health monitoring.
- Domain Name System Security Extensions (DNSSEC) support.
- Backup improvements.
- The following Virtual Service application configuration templates were published:
    - DNS
    - Ellucian Luminis Portal
    - NGINX server
    - Aspera Server
    - TFTP
    - Microsoft Print Server
    - Graylog server

9.2 Feature Enhancements

- Allow TLS version selection for re-encryption.
- Allow explicitly trusting of self-signed or untrusted Real Server certificates.
- Updated the kernel to mitigate against the CVE-2016-5195 vulnerability.
- PowerShell/API enhancements:
    - SSO session monitoring
    - HA status
    - GEO partner status

- Certificate management

- Licensing

- LDAP authentication now supports search scope and Bind DN.
- LDAP query for group membership (for NTLM).
- You can set a different syslog destination port when using remote syslog servers.
- TLS1.1 and TLS1.2 are the default encryption protocols.
- Support for OCSP stabling for certificate-based client authentication.
- ESP support for password expiry detection and display of link to change.
- There is greater visibility and control over the sessions being authenticated using ESP.
- You can use Security Identifiers (SIDs) instead of canonical names for Permitted Groups in ESP.
- All LoadMasters for Azure and Amazon Web Services (AWS) have unique serial numbers.
- Updated the OpenSSL version to 1.0.2k to mitigate against the following vulnerabilities:

  - CVE-2017-3731

  - CVE-2017-3730

  - CVE-2017-3732

  - CVE-2016-7055

  - CVE-2016-9131

  - CVE-2016-9147

  - CVE-2016-9444

  - CVE-2016-9778

9.3 Issues Resolved

PD-8417	Removed brackets from X-Forwarded-For header.
PD-7676	Increased PCRE limit from 1500 to 3000.
PD-8010	Improved error message that appears when trying to create a Web Application Firewall (WAF) Virtual Service and the limit of WAF Virtual Services has already been reached.

PD-8339	Enhancements made to WAF-enabled templates.
PD-8596	Error log is no longer generated on a successful FTP automated backup.
PD-8559	Removal of popup message when viewing log files.
PD-8531	The Disable Password Form setting is working with custom image sets.
PD-8453	Fixed an issue with FTP backups.
PD-8451	Fixed an issue which caused a segfault in certain scenarios.
PD-8439	Fixed an issue that reported errors in the logs after upgrading the firmware version on the VLM-1000 model.
PD-8407	Fixed an issue which prevented the ESP client from authenticating locked users.
PD-8371	ESP SubVS connection logs show Real Servers.
PD-8341	The MTU size is no longer getting reset to 1500 when bonding interfaces together.
PD-8298	Fixed some issues relating to IPv6 routing.
PD-8285	Some JavaScript appearing in the LoadMaster warn logs is being executed by the browser.
PD-8281	Resolved issue with IP address assignment in Azure multi-arm deployments.
PD-8205	Fixed some issues with content rules matching multiple requests on the same connection.
PD-8200	It is possible to manage admin certificates from the individual IP addresses of a HA pair.
PD-8101	Fixed SAML response issue.
PD-8097	Fixed some issues with accessing WebSocket when using Firefox and a LoadMaster.
PD-8085	Fixed an issue that was un-setting the admin certificate for the Web User Interface (WUI) when modifying a VLAN interface.
PD-8025	Graphs showing information when SDN add-on is enabled.
PD-8006	Fixed an issue with the “everywhere” option when using location-based selection criteria.

PD-7789	Fixed an issue that caused high CPU utilization when using the Web Application Firewall (WAF) in certain situations.
PD-7778	Fixed an issue that was causing the SSL open/opening connections limit to be reached in certain circumstances, even though there were only a few connections running.
PD-8597	Fixed an issue which was causing a segfault in certain situations.
PD-8463	Fixed an issue which was preventing the Critical option from being set on SubVS health checks.
PD-8399	Fixed API command code failure for L7 Connection Drain Time (secs).
PD-8320	Fixed an issue where the SDN add-on was not passing the username and password to the HP SDN controller.
PD-8072	Fixed an issue which prevented the importing of exported templates.
PD-8430	Fixed LDAP endpoint behaviour for multiple servers.
PD-8372	Fixed an issue with disabling SSO domain LDAP health checks.
PD-8282	Fixed an issue which was causing the system to constantly report disk errors.
PD-8114	Fixed an issue that reported an incorrect Virtual Service status when using ESP and the LDAP StartTLS health check fails.
PD-8030	Fixed an issue which returned SNMP details even when SNMP was disabled.
PD-8225	The correct error message is displayed when incorrect credentials are used when licensing the LoadMaster.
PD-8552	Fixed a permissions issue which prevented users with Virtual Service permissions from changing the Virtual Service IP address and port.
PD-8086	AWS Virtual LoadMasters (VLMs) now have session management enabled.
PD-7998	Improved handling of admin WUI parameters.
PD-8112	Fixed an issue which caused SSL re-encrypt to not function with Sorry Servers as expected.
PD-8397	GEO clusters checking a Virtual Service that uses enhanced health checks reports a down status correctly.
PD-8296	Allowed vRealize Operations/Orchestrator Manager to be configured for a

	custom management port.
PD-8549	Fixed UI permissions for adding/deleting templates.
PD-8083	Added new PowerShell API commands to get/set the cluster HA mode.
PD-8005	Fixed issues with the PowerShell API that were causing errors with Microsoft Service Management Automation (SMA).
PD-8192	Removed unnecessary output from the Get-NetworkDNSConfiguration API command.
PD-7559	It is possible to add a comment to a block or whitelist entry in the Access Control List (ACL) when using the API.
PD-8555	The Virtual Service status is listed in the stats API command.
PD-8525	It is possible to set some parameter values to null using the Set-LmParameter PowerShell API command.
PD-8307	Improved the licenseinfo API command to report TPS and throughput limits.
PD-8305	Fixed failure message for the aslactivate API command.
PD-8168	Fixed an issue with setting the High Availability (HA) mode using the API.
PD-8164	Removed the credentials and LoadMaster port parameters from the PowerShell cmdlets URL.
PD-8080	Removed unnecessary output from the Get-HAOption PowerShell API command.
PD-8043	Improved the error when saving a file as a result of a PowerShell API command does not work.
PD-8031	Added the LoadMaster HTTP port parameter to commands that were missing it.
PD-7909	Improved error handling for the Set-GeoFQDN PowerShell API command.
PD-8515	Fixed an issue which caused an error when using the FQDN for the LoadBalancer parameter on certain PowerShell API commands.
PD-8233	It is possible to set the persistence mode to none when creating a new Virtual Service using the PowerShell API.
PD-8365	Fixed an issue which was causing the RESTful API show domain command to list domain values even when a non-existing domain name was

	specified.
PD-8363	Fixed an issue which prevented the getall API command from returning details if HA was not configured.
PD-8358	Added success responses for the Add/Remove Cache/Compression PowerShell API commands.
PD-8346	Added a delay for some PowerShell API commands to prevent the LoadMaster from closing the connection.
PD-8236	Fixed a typo in the license API commands.
PD-8009	The listcluster API command returns a status.
PD-7990	Improved response for the Set-SecAdminAccess API command.
PD-7958	Improved error handling for the New-NetworkRoute PowerShell API command.
PD-7957	Fixed an issue with the Set-NetworkInterface PowerShell API command.
PD-7956	Fixed an issue with the set networking PowerShell API commands.
PD-7863	Fixed an issue where the RESTful API was not displaying the Disable JSON Parser and Disable XML Parser options when Inspect HTML Post Request Content is enabled.
PD-7856	Fixed an issue with the RESTful API where NAT functionality did not work in a specific scenario.
PD-7742	Made DNS query maximum field length value consistent in both the WUI and API (126-character maximum).
PD-7487	Improved return message for addlocaluser and usersetperms API commands.
PD-7338	The listclusters API command returns the correct health check port value.
PD-6817	Made behaviour consistent between WUI and API when creating new Virtual Services for Azure VLMs.
PD-8038	The showcluster API command returns the correct status value.
PD-8290	Fixed an issue that caused browsers to execute JavaScript from warning logs.

9.4 Known Issues

PD-10980	A critical vulnerability in the LoadMaster Operating System (LMOS) related to Session Management could allow an unauthorized, remote attacker to bypass security protections, gain system privileges, and execute elevated commands such as **ls**, **ps**, **cat**, and so on, thereby compromising the system. Through this remote execution, in certain cases, exposure of sensitive system data such as certificates, private keys, and other information may be possible. Further information can be found here: Mitigation For Remote Access Execution Vulnerability.
PD-9892	**Application of SNORT rules does not work.**
PD-10155	Issue with configuration corruption causes some GEO features not to function.
PD-8771	When using SAML, users are being directed to the IdP SSO URL instead of the IdP Logoff URL when logging off.
PD-8760	The LoadMaster is displaying a message saying the WAF rulesets are out-of-date when in some cases, they are not.
PD-8730	In some cases, clients are unable to authenticate using ESP.
PD-8746	Issues downloading/installing WAF rules after doing a factory reset.
PD-8413	Cannot specify wildcard port when creating a Virtual Service from a template.
PD-8766	"Everywhere" shows up twice in location selection.
PD-8725	Proximity and Location Based scheduling does not work with IPv6 source addresses.
PD-8014	A remote LoadMaster cluster does not respond unless the remote LoadMaster has a Virtual Service.
PD-8357	Minor issue with error handling when adding a new cluster using the API.
PD-8196	When using the enablewafremotelogging API command it is possible to set the remote URI to an invalid format.

PD-8118	The GEO Update Interface cannot be set using the API.
PD-7613	The showiface and modiface API commands do not show the User for Cluster Checks and Use for Cluster Updates options.
PD-7156	The VS index parameter is missing from some API commands.
PD-8378	The listvs command fails incorrectly when given bad data.
PD-8716	Locked users are displayed in a format which is not easily readable when running the showdomainlockedusers API command.
PD-8561	No response received when running the createbond/unbond API commands, even when they are successful.
PD-8649	When /tmp is partially full (~17%), the LoadMaster is unable to apply a firmware patch using the API.
PD-10160	The API commands to reset the CPU and network graphs do not work.

10 Release 7.2.36.2

Refer to the sections below for details about firmware version 7.2.36.2. This was released on 14th December 2016.

10.1 Issues Resolved

PD-8479	Resolved issues where Virtual Services (VS) were wrongly deleted from the LoadMaster.
PD-8480	Fixed an issue that was causing high Web Application Firewall (WAF) CPU usage.

10.2 7.2.36.2 - Known Issues

PD-10980	A critical vulnerability in the LoadMaster Operating System (LMOS) related to Session Management could allow an unauthorized, remote attacker to bypass security protections, gain system privileges, and execute elevated commands such as **ls**, **ps**, **cat**, and so on, thereby compromising the system. Through this remote execution, in certain cases, exposure of sensitive system data such as certificates, private keys, and other information may be possible. Further information can be found here: Mitigation For Remote Access Execution Vulnerability.
PD-8725	**Proximity** and **Location Based** scheduling do not work with IPv6 source addresses.
PD-9950	LoadMaster VNF HA does not work on LoadMaster versions 7.1.35.*n* and 7.2.36.*n*. It does work om LoadMaster version 7.2.37 and above.
PD-9892	**Application of SNORT rules does not work.**
PD-10155	Issue with configuration corruption causes some GEO features not to function.
PD-10160	The API commands to reset the CPU and network graphs do not work.

11 Release 7.2.36.1

Refer to the sections below for details about firmware version 7.2.36.1. This was released on 17th November 2016.

11.1 New Features

The following features were added to the 7.2.36.1 release:

- Unified Capabilities Approved Product List (UC APL) updates
- The following Virtual Service application configuration templates were published:
  - IBM Domino
  - RabbitMQ
  - Epic Medical Systems
  - Pearson PowerSchool
  - vSphere Platform Service Controllers (PSC)
  - Apache Tomcat
  - Apache HTTP
  - Horizon View 7.0
  - Microsoft IIS
- LoadMaster kernel update
- Additional Dell support
- Security Assertion Markup Language (SAML)-based authentication Proof of Concept (PoC)
- License type selection
- Digital signing of PowerShell Application Program Interface (API) module
- Certificate-based authentication added for the PowerShell API module

11.2 Feature Enhancements

- Enhanced special character handling for form-based Edge Security Pack (ESP) logins.
- Active File Transfer Protocol (FTP) traffic is being Network Address Translated (NATed) to the expected IP address.

- Updated the OpenSSL version to 1.0.2j.
- Updated the BIND version on the LoadMaster to 9.10.4-P3 to mitigate against the CVE-2015-5722 and CVE-2015-5986 vulnerabilities.
- Support added for Dell Broadwell hardware.
- Enhancements made to the debug checks performed when licensing fails.
- On newly created Virtual Services, transparency is disabled and Subnet Originating Requests is enabled by default.
- Improvements made to eliminate the possibility of having duplicate High Availability (HA) Virtual IDs.
- Three days after deploying a LoadMaster for Amazon Web Services (AWS), you are prompted to type your KEMP ID and password to activate your support subscription.
- Lightweight Directory Access Protocol (LDAP) health checks added.
- A header value can be copied into a custom header.
- Support added for the ModSecurity JavaScript Object Notation (JSON) log format.
- It is possible to configure the check port for the DNS health check type in the Web User Interface (WUI).
- SSL certificates, SSO settings and associated settings are now synchronized between cloud-based HA pairs.
- Added an API command to check the previous firmware version.
- The showiface API command now lists all interfaces if an interface is not specified.
- A number of diagnostic commands added to the PowerShell API module.

11.3 Issues Resolved

PD-7975	The newest USB drivers for keyboards are supported.
PD-7807	Fixed an issue that was causing the LoadMaster to crash in a specific scenario.
PD-7770	Fixed some issues relating to the GEO proximity Selection Criteria.
PD-7376	Subnet Originating Requests are now respected when the LoadMaster is using a “Sorry” Server.
PD-7939	Fixed an issue that was displaying incorrect Real Server statistics.

PD-7845	It is possible to assign multiple Web Application Firewall (WAF) rules to a Virtual Service using the API.
PD-8004	Fixed an issue with the Real Server icons.
PD-7946	Fixed an issue that caused a reboot loop on Hyper-V with the Intel Skylake processor.
PD-7937	A notification is displayed when the GEO cluster limit is reached.
PD-7915	Fixed an issue with historical graphs.
PD-7787	Fixed an issue with cloud HA synchronization.
PD-7747	Fixed an issue that was causing GEO partner updates to fail.
PD-7738	Stopped a spurious log message from appearing.
PD-7729	Rectified a truncation issue with LinOTP-2 factor PIN.
PD-7726	Fixed an issue that prevented exported templates from working when Detect Malicious Requests is enabled.
PD-7713	Fixed an issue that was causing the health check status to show as unchecked in Azure HA units (even though the health check probe was working correctly).
PD-7678	Fixed an issue that locked out some LoadMaster users when using HA and session management.
PD-7578	Fixed an issue that prevented wildcard UDP Virtual Services from NATing the return traffic as expected.
PD-7757	Fixed an issue that prevented ciphers being selected in the Microsoft Edge and Internet Explorer browsers.
PD-7643	Fixed an issue that was causing the LoadMaster to enter passive mode after rebooting three times without the LoadMaster being up for more than five minutes.
PD-7617	Made improvements to the boot log to make it easier to read.
PD-7752	Improved RADIUS challenge-OTP handling.
PD-7696	It is possible to set the Checked Port using the API.
PD-7556	It is possible to set the Persistence Mode to none using the PowerShell API.
PD-7753	Fixed an issue that required the port to be specified when running the

	Enable-SecAPIAccess and Disable-SecAPIAccess commands.
PD-7658	Fixed an issue that prevented the netsonsole parameter from being set using the PowerShell API.
PD-7656	Fixed an issue preventing certain values from being unset using the Set-SecRemoteAccess PowerShell API command.
PD-7650	Corrected the API command for WAF commercial rule updates and installations.
PD-7648	Fixed an issue preventing a custom rule data file from being uploaded using the RESTful API.
PD-7608	It is possible to enable the Require SNI hostname flag using API commands.
PD-7540	Fixed a misspelling in a RESTful API command.
PD-7522	Improved error handling for API commands relating to GEO maps.
PD-7516	It is possible to set the GEO location of "everywhere" using the API.
PD-7565	The checker address can be set using the API.

11.4 Known Issues

PD-10980	A critical vulnerability in the LoadMaster Operating System (LMOS) related to Session Management could allow an unauthorized, remote attacker to bypass security protections, gain system privileges, and execute elevated commands such as **ls**, **ps**, **cat**, and so on, thereby compromising the system. Through this remote execution, in certain cases, exposure of sensitive system data such as certificates, private keys, and other information may be possible. Further information can be found here: Mitigation For Remote Access Execution Vulnerability.
PD-8725	**Proximity** and **Location Based** scheduling do not work with IPv6 source addresses.
PD-9892	**Application of SNORT rules does not work.**
PD-9950	LoadMaster VNF HA does not work on LoadMaster versions 7.1.35.*n* and 7.2.36.*n*. It does work om

	LoadMaster version 7.2.37 and above.
PD-10155	Issue with configuration corruption causes some GEO features not to function.
PD-8371	ESP SubVS connection logging is not showing Real Servers.
PD-8341	The MTU size is getting reset to 1500 when bonding interfaces together.
PD-8298	There are some issues relating to IPv6 routing.
PD-8285	Some JavaScript appearing in the LoadMaster warn logs is being executed by the browser.
PD-8205	There are some issues with content rules matching multiple requests on the same connection.
PD-8200	It is not possible to manage admin certificates from the individual IP addresses of a HA pair.
PD-8297	The vRealize Operations Manager Adapter setup fails if the API is disabled.
PD-8296	When using the vRealize Operations Manager, the management port must be set to 443 otherwise it fails.
PD-8399	The WUI help text says it is possible to set the L7 Connection Drain Time to 0 but this is not possible. Valid values range between 60 and 86400.
PD-8192	There is some unnecessary output from the Get-NetworkDNSConfiguration API command.
PD-9089	In some cases, after upgrading the LoadMaster firmware from version 7.1.35 to a newer firmware version, historical graphs may not display. To fix this, reset the statistic counters (**System Configuration > Logging Options > System Log Files > Debug Options > Reset Statistics**).
PD-10160	The API commands to reset the CPU and network graphs do not work.

12 Release 7.1.35.5 (Long Term Support)

Refer to the sections below for details about firmware version 7.1.35.5. This was released on 22nd March 2018.

12.1 7.1.35.5 - New Features

The following feature was added to the 7.1.35.5 release:

- Added support for the new LM-X series of LoadMaster hardware.

12.2 7.1.35.5 - Feature Enhancements

- The LTS build is now available in the Azure Marketplace.
- Updated the Copyright Notices on the LoadMaster console and Web User Interface (WUI).

12.3 7.1.35.5 - Issues Resolved

PD-11023	Previously, a critical vulnerability in the LoadMaster Operating System (LMOS) related to Session Management could allow an unauthorized, remote attacker to bypass security protections, gain system privileges, and execute elevated commands such as **ls**, **ps**, **cat**, and so on, thereby compromising the system. Through this remote execution, in certain cases, exposure of sensitive system data such as certificates, private keys, and other information may be possible. Now, this vulnerability has been mitigated against with more stringent security checks. Further information can be found here: Mitigation For Remote Access Execution Vulnerability.

12.4 7.1.35.5 - Known Issues

PD-10241	Unable to patch upgrade using the Application Program Interface (API) to newer versions of the LoadMaster.
PD-10138	Only text/XML and application/JSON content types are supported with the **Inspect HTML POST Request Content** feature.
PD-10192	The LoadMaster is unable to set up an IPsec tunnel to Azure classic/Azure Resource Manager (ARM) endpoints.
PD-10187	Web Application Firewall (WAF) statistics do not get reset on Virtual Service deletion.
PD-10184	An issue exists which prevents some users from accessing some Virtual Services when using WAF.

PD-10183	WAF does not block the response, even when the **Process Responses** option is enabled on the Virtual Service.
PD-10182	Enabling WAF on a Virtual Service with no rules applied causes a specific web feature to fail.
PD-10181	When an HTTP response contains a status of **HTTP/1.1 500 Internal Server Error** and the location header is populated, the response to the client is dropped and the client sees nothing.
PD-10180	High CPU utilization can be seen when using WAF in certain situations.
PD-9976	An issue occurs preventing Layer7 from initializing when processing SNORT rules.
PD-9953	A security issue exists causing the initial boot password to be written in the Azure Virtual LoadMaster logs.
PD-9777	Issues can occur when using the license API if the timezone on the LoadMaster is set to GMT-X.
PD-9950	LoadMaster VNF HA does not work on LoadMaster versions 7.1.35.*n* and 7.2.36.*n*. It does work on LoadMaster version 7.2.37 and above.
PD-10155	Issue with configuration corruption causes some GEO features not to function.
PD-9901	HA does not work with LTS VNF 7.1.35.4 on the Multi-Tenant LoadMaster.
PD-9770	ESP logs missing some information.
PD-9743	Issues importing some template files that have the default rule assigned.
PD-9666	Headers with underscores are not accepted by Apache 2.4.
PD-9660	The LoadMaster is changing RADIUS passwords in some scenarios.
PD-9633	Unable to set the check host with the port attached in the WUI (it works using the API or CLI).
PD-9517	Unable to authenticate some users when the password is expired and permitted groups are used.
PD-9508	ESP only verifies SAML assertions when using the root certificate.
PD-9504	Some users are experiencing issues with HA failover on Multi-Tenant LoadMaster units.
PD-10159	CPU and network usage graphs not appearing after firmware upgrade. Resetting the statistic counters does not clear the graph data.

PD-9470	LDAP Real Server health checking is not working optimally.
PD-9453	Some Azure users are having issues licensing due to communication issues with the default gateway.
PD-9359	Some users unable to authenticate using ESP.
PD-9159	When WAF is enabled there is no traffic on the back-end in certain scenarios.
PD-8697	Some users having issues detecting the partition when using the Hardware Security Module (HSM).
PD-9768	Security issue in the SSO debug logs relating to the logon transcode option.
PD-9657	Naming a cipher set using **-** or **+** results in some issues.
PD-9643	Unable to change the IP address of a Virtual Service in an Azure LoadMaster.
PD-9604	Issues when trying to import some custom templates.
PD-9783	HA status tool tip on slave unit displays incorrect IP addresses.
PD-9758	Some users are unable to edit or access Office files from SharePoint when using SAML and KCD authentication.
PD-7157	When using WAF and KCD, all file attachments in SharePoint fail.
PD-7265	No redirection when the shared IP address is changed using the WUI.
PD-8746	If a LoadMaster licensed with WAF rules has had rules downloaded/installed and then a factory reset is performed, it is not possible to download/install WAF rules.
PD-8413	It is not possible to specify a wildcard port when creating a Virtual Service from a template.
PD-9129	The API command to backup contains an error that breaks the PowerShell wrapper connection.
PD-9779	Discrepancies between the WUI and RESTful API parameter for "Client Authentication Mode".
PD-9596	The **showiface** RESTful API command shows the wrong interface values in the output for interfaces that are not configured.
PD-9572	There are discrepancies displaying the location latitude/longitude parameter values for some RESTful API commands.
PD-9570	There is a typo in the **removecountry** API response error message.
PD-9553	There is no API command to disable secure NTP mode.

PD-9539	Issues with the PowerShell **New-GeoCluster** command in a specific scenario.
PD-9525	The RESTful API returns the value of the **failtime** parameter in seconds, but it is set in minutes.
PD-9523	In a specific scenario, the RESTful API returns a success message when fetching a non-existing GEO FQDN.
PD-9476	There is no RESTful API command to get/list the installed custom rule data files.
PD-7156	The **VSIndex** parameter is missing in some API calls.
PD-9575	There are issues with some **aclcontrol** API commands.
PD-10160	The API commands to reset the CPU and network graphs do not work.

13 Release 7.1.35.4

Refer to the sections below for details about firmware version 7.1.35.4. This was released on 2nd August 2017.

13.1 7.1.35.4 - Feature Enhancements

- Updated OpenSSH to version 7.5p1
- Improvements made to support a high number of connections.

13.2 7.1.35.4 - Issues Resolved

PD-9678	Fixed an issue that was causing there to be no back-end traffic when the Web Application Firewall (WAF) was enabled.
PD-9650	Fixed an issue that was causing WAF to block the uploading of files larger than 1MB.
PD-9631	It is possible to modify the IP address of the shared IP on a VLAN interface.
PD-9438	Fixed an issue with the **Drop Connections on RS failure** that caused high RAM usage.
PD-9353	Fixed an issue that caused the LoadMaster to reboot when the persistence mode of a UDP syslog Virtual Service was changed.
PD-9352	Fixed an issue that caused simultaneous health check failures.
PD-9333	Removed "deprecated option" SSO manager logs.
PD-9769	Fixed a security issue with the SSO debug logs relating to the logon transcode option.
PD-9637	Mitigated against the CVE-2017-8890 vulnerability.
PD-9756	Fixed an issue with certificate authentication when using a HA pair.
PD-9569	Fixed an issue with special space characters and local LoadMaster user authentication.
PD-9806	Fixed an issue with some **aclcontrol** API commands.
PD-9790	The **CheckPort** and **CheckPattern** API parameters can be unset using the API.
PD-9773	Fixed an issue that showed different statuses for disabled Virtual Services in the API.

13.3 7.1.35.4 - Known Issues

PD-11023	A critical vulnerability in the LoadMaster Operating System (LMOS) related to Session Management could allow an unauthorized, remote attacker to bypass security

	protections, gain system privileges, and execute elevated commands such as **ls**, **ps**, **cat**, and so on, thereby compromising the system. Through this remote execution, in certain cases, exposure of sensitive system data such as certificates, private keys, and other information may be possible. Further information can be found here: Mitigation For Remote Access Execution Vulnerability.
PD-9950	LoadMaster VNF HA does not work on LoadMaster versions 7.1.35.*n* and 7.2.36.*n*. It does work on LoadMaster version 7.2.37 and above.
PD-10155	Issue with configuration corruption causes some GEO features not to function.
PD-9901	HA does not work with LTS VNF 7.1.35.4 on the Multi-Tenant LoadMaster.
PD-9770	ESP logs missing some information.
PD-9743	Issues importing some template files that have the default rule assigned.
PD-9666	Headers with underscores are not accepted by Apache 2.4.
PD-9660	The LoadMaster is changing RADIUS passwords in some scenarios.
PD-9633	Unable to set the check host with the port attached in the WUI (it works using the API or CLI).
PD-9517	Unable to authenticate some users when the password is expired and permitted groups are used.
PD-9508	ESP only verifies SAML assertions when using the root certificate.
PD-9504	Some users are experiencing issues with HA failover on Multi-Tenant LoadMaster units.
PD-10159	CPU and network usage graphs not appearing after firmware upgrade. Resetting the statistic counters does not clear the graph data.
PD-9470	LDAP Real Server health checking is not working optimally.
PD-9453	Some Azure users are having issues licensing due to communication issues with the default gateway.
PD-9359	Some users unable to authenticate using ESP.
PD-9159	When WAF is enabled there is no traffic on the back-end in certain scenarios.
PD-8697	Some users having issues detecting the partition when using the Hardware Security Module (HSM).
PD-9768	Security issue in the SSO debug logs relating to the logon transcode option.
PD-9657	Naming a cipher set using **-** or **+** results in some issues.

PD-9643	Unable to change the IP address of a Virtual Service in an Azure LoadMaster.
PD-9604	Issues when trying to import some custom templates.
PD-9783	HA status tool tip on slave unit displays incorrect IP addresses.
PD-9758	Some users are unable to edit or access Office files from SharePoint when using SAML and KCD authentication.
PD-7157	When using WAF and KCD, all file attachments in SharePoint fail.
PD-7265	No redirection when the shared IP address is changed using the WUI.
PD-8746	If a LoadMaster licensed with WAF rules has had rules downloaded/installed and then a factory reset is performed, it is not possible to download/install WAF rules.
PD-8413	It is not possible to specify a wildcard port when creating a Virtual Service from a template.
PD-9129	The API command to backup contains an error that breaks the PowerShell wrapper connection.
PD-9779	Discrepancies between the WUI and RESTful API parameter for "Client Authentication Mode".
PD-9596	The **showiface** RESTful API command shows the wrong interface values in the output for interfaces that are not configured.
PD-9572	There are discrepancies displaying the location latitude/longitude parameter values for some RESTful API commands.
PD-9570	There is a typo in the **removecountry** API response error message.
PD-9553	There is no API command to disable secure NTP mode.
PD-9539	Issues with the PowerShell **New-GeoCluster** command in a specific scenario.
PD-9525	The RESTful API returns the value of the **failtime** parameter in seconds, but it is set in minutes.
PD-9523	In a specific scenario, the RESTful API returns a success message when fetching a non-existing GEO FQDN.
PD-9476	There is no RESTful API command to get/list the installed custom rule data files.
PD-7156	The **VSIndex** parameter is missing in some API calls.
PD-9575	There are issues with some **aclcontrol** API commands.
PD-10160	The API commands to reset the CPU and network graphs do not work.

14 Release 7.1.35.3

Refer to the sections below for details about firmware version 7.1.35.3. This was released on 5th April 2017.

14.1 Feature Enhancements

- Updated OpenSSH version to 7.4p1.
- Updated OpenSSL version to 1.0.2k to mitigate against the following vulnerabilities:

  - CVE-2017-3731

  - CVE-2017-3730

  - CVE-2017-3732

  - CVE-2016-7055

- Updated BIND to version 9.10.4-P5 to mitigate against the following vulnerabilities:

  - CVE-2016-9131

  - CVE-2016-9147

  - CVE-2016-9444

  - CVE-2016-9778

- Updated the Copyright Notices on the LoadMaster console and Web User Interface (WUI).
- Support added for OWASP CRS 3.0 rules.

14.2 Issues Resolved

PD-9042	Removed brackets from IPv6 X-Forwarded-For header.
PD-8643	Increased the connection levels that cause local port exhaustion.
PD-8982	Added an option to not include netstat in backups.
PD-9075	Fixed some session management issues.
PD-8996	Fixed an issue that was causing the SSL open/opening connections limit to be reached incorrectly.

PD-8777	Fixed an issue that prevented clients from authenticating using the Edge Security Pack (ESP) in certain scenarios.
PD-8717	Fixed an issue relating to the ESP Locked_users file.
PD-8569	Stopped an unnecessary error message from being displayed when viewing log files.
PD-9120	The Virtual Service status is listed in the stats Application Program Interface (API) command.

14.3 Known Issues

PD-11023	A critical vulnerability in the LoadMaster Operating System (LMOS) related to Session Management could allow an unauthorized, remote attacker to bypass security protections, gain system privileges, and execute elevated commands such as **ls**, **ps**, **cat**, and so on, thereby compromising the system. Through this remote execution, in certain cases, exposure of sensitive system data such as certificates, private keys, and other information may be possible. Further information can be found here: Mitigation For Remote Access Execution Vulnerability.
PD-8725	**Proximity** and **Location Based** scheduling do not work with IPv6 source addresses.
PD-9950	LoadMaster VNF HA does not work on LoadMaster versions 7.1.35.*n* and 7.2.36.*n*. It does work on LoadMaster version 7.2.37 and above.
PD-10159	CPU and network usage graphs not appearing after firmware upgrade. Resetting the statistic counters does not clear the graph data.
PD-8009	The listcluster API command does not return a status.
PD-8298	There are some issues relating to IPv6 routing.
PD-8097	There are some issues accessing WebSocket when using Firefox and a LoadMaster.
PD-8005	There are issues with the PowerShell API that are causing errors with Microsoft Service Management Automation (SMA).
PD-8341	The MTU size is getting reset to 1500 when bonding interfaces.
PD-8305	The aslactivate API command always returns a success message even when the activation fails.

PD-8192	The Get-NetworkDNSConfiguration API command returns High Availability (HA) parameters, even when the LoadMaster is not in HA mode.
PD-7778	In some circumstances, the SSL open/opening connections limit is reached, even though there are only a few connections running.
PD-7559	It is not possible to add a comment to a block or whitelist entry in the Access Control List (ACL) when using the API.
PD-8196	There is no validation of the remote URI when enabling WAF logging using the API.
PD-8174	Clusters with a forward slash (/) in the name do not show up in the WUI.
PD-8107	It is not possible to force an NTP update using the API.
PD-8038	In some scenarios, the API is not returning the correct value for the cluster status.
PD-8014	A remote LoadMaster cluster does not respond unless the remote LoadMaster has a Virtual Service.
PD-8225	An incorrect error message is displayed when incorrect credentials are used when licensing the LoadMaster.
PD-8205	When using content rules, the LoadMaster does not match the port when trying to select a Real Server.
PD-7487	When adding a local user and the name of the user is bal, the response is correct but the response stat is invalid – it should be 400/422 or another stat, but not 200.
PD-10160	The API commands to reset the CPU and network graphs do not work.

15 Release 7.1.35.2

Refer to the sections below for details about firmware version 7.1.35.2. This was released on 9th November 2016.

15.1 Issues Resolved

PD-8290	Fixed an issue that was causing browsers to execute JavaScript from warning logs.
PD-8240	Fixed an issue with IP assignment in Azure multi-arm LoadMasters.
PD-8193	Fixed a display issue with statistics.
PD-8189	Fixed an issue that allowed unauthorized API commands to be run.
PD-8188	Fixed an issue that caused errors to appear in the Virtual Service when no Web Application Firewall (WAF) rules were assigned.
PD-8187	Updated BIND to version 9.10.4-P3.

15.2 7.1.35.2 - Known Issues

PD-11023	A critical vulnerability in the LoadMaster Operating System (LMOS) related to Session Management could allow an unauthorized, remote attacker to bypass security protections, gain system privileges, and execute elevated commands such as **ls**, **ps**, **cat**, and so on, thereby compromising the system. Through this remote execution, in certain cases, exposure of sensitive system data such as certificates, private keys, and other information may be possible. Further information can be found here: Mitigation For Remote Access Execution Vulnerability.
PD-8725	**Proximity** and **Location Based** scheduling do not work with IPv6 source addresses.

16 Release 7.1.35

Refer to the sections below for details about firmware version 7.1.35. This was released on 2nd August 2016.

When upgrading a LoadMaster for Microsoft Azure to firmware version 7.1.35 – you must upgrade the Azure add-on pack first.

16.1 New Features

The following features were added to the 7.1.35 release:

- Multiple logoff strings can be specified.
- Real Servers can be referenced by Fully Qualified Domain Name (FQDN) or IP address.
- The LoadMaster can Network Address Translate (NAT) IPv6 traffic.
- The following Virtual Service application configuration templates were published:
  - VMware vRealize Automation
  - Microsoft Dynamics AX
  - JBoss Application Server
  - Remote Desktop Services
  - AirWatch
  - Splunk
  - Syncplicity
- The Microsoft Exchange, SharePoint and IIS application configuration templates are updated.
- GEO supports blacklists.
- The standard Linux/Unix utility **du was** added to the LoadMaster Operating System (OS).
- An Azure Resource Manager (ARM) basic setup template for High Availability (HA) is available.
- Closed network licensing.
- New public cloud WAF products.
- Enhanced IPv6 ping support.
- GEO per-FQDN settings.
- Enhanced GEO health checks to enable grouping by cluster.

- It is possible to perform a TCP dump by using the Application Program Interface (API).

16.2 Feature Enhancements

- Improved client certificate Common Name (CN) handling.
- Updated default values for SecRequestBodyNoFilesLimit and SecRequestBodyInMemoryLimit to 1048576.
- Improved Subject Alternative Name (SAN) handling with multiple Virtual Service certificates.
- It is possible to configure timeouts for Single Sign On (SSO) token authentication.
- Updated the OpenSSH version to 7.2p2.
- It is possible to enable and disable individual WAF rules in each ruleset.
- Product and service support types and dates are listed under the **View License** link on the Web User Interface (WUI) home page.
- Improved WAF rules auto-download behaviour.
- Session management is enabled by default on new LoadMasters.
- ModSecurity has been updated to version 2.9.
- Enhanced API functionality for the command to list all installed templates.
- The PowerShell API cmdlets have been renamed to follow Microsoft naming conventions. Previous naming conventions have been retained for backwards compatibility.

16.3 Issues Resolved

PD-6879	Improved handling of SAMAccountName/User Principal Name (UPN) in multiple domain environments.
PD-7668	Added an option to set HTTPlib timeout for SDNstats to the LoadMaster WUI.
PD-7564	Fixed an issue which was preventing the selection of the UDP Session Initiation Protocol persistence method.
PD-7476	Fixed an issue where some statistics were disappearing in certain scenarios.
PD-7467	Fixed an issue which was preventing historical statistics from appearing.
PD-7464	The LoadMaster continues as expected after a successful LDAP bind when using alternative domains.
PD-7331	The spelling error has been corrected in the Français Canadien Blank SSO

	image set.
PD-7222	WAF event logs are exported to syslog.
PD-7153	Fixed some strange licensing behaviour for SPLA Virtual LoadMasters.
PD-7141	The grave character (`) is supported in ESP passwords.
PD-6889	Enhanced HA mode settings behaviour when one node is down.
PD-7617	The boot log no longer refreshes and scrolls to the bottom of the page, making it easier to read.
PD-7609	Increased the dhcpcd timeout to accommodate for some hardware Network Interface Controllers (NICs).
PD-7173	Fixed issues relating to pre-authorization excluded directories and Kerberos Constrained Delegation (KCD)
PD-7127	The Kerberos cache is purged cleanly.
PD-7099	Fixed an issue which was preventing SubVSs from being created within a Log Insight Virtual Service in certain situations.
PD-7047	Fixed an issue with Name Server (DNS) protocol health checking.
PD-7226	Longer comments are allowed in templates to better support older templates.
PD-7121	OCSP responses containing multiple certificates are processed correctly.
PD-7056	Fixed an issue relating to black list IP addresses in Virtual Services.
PD-7128	The persist parameter is appearing in the showvs API command output in all situations.
PD-7119	Path MTU Discovery (PMTUD) notifications are no longer ignored when the packet filter is enabled.
PD-7080	Fixed an issue which was causing the IPv6 default route to be lost after High Availability (HA) failover.
PD-7481	Fixed an issue relating to incorrect site selection failover when using Location Based as the Selection Criteria.
PD-7512	Removed some spurious error messages from the LoadMaster WUI.
PD-7475	Corrected the message which is displayed to the user after downloading WAF rules.
PD-7339	Fixed an issue with the Disable Password Form option in Firefox browsers.

PD-7134	Fixed the GEO LoadMaster WUI to display missing menu elements.
PD-7076	Fixed issues with NAT functionality which was not working as expected in a specific scenario.
PD-7011	Improved warning messages when a user is trying to delete or block themselves.
PD-6548	Resolved an issue which was causing high CPU usage after additional services were added.
PD-7021	There is no longer a discrepancy between the length of the Add Header to Request field between the WUI and API.
PD-7014	Fixed an issue relating to the removal of extra ports using the PowerShell API.
PD-7582	Enhancements have been made to the PowerShell commands to enable and disable the API.
PD-7217	Enhancements have been made to the Java modify interface command.
PD-7637	Fixed an issue with the PowerShell Initialize-Loadbalancer command.
PD-7023	Improved error handling for the Get-Rule API command.
PD-7016	Fixed an issue which was preventing the “Include query” flag from being set for a content rule using the PowerShell API.
PD-7184	The showrs RESTful API command returns the correct VSIndex value.
PD-7642	Fixed a typo in the PowerShell API command New-TlsintermediateCertificate.
PD-7541	Fixed an issue which was preventing the showiface API command from working with clustering.
PD-7509	It is possible to set the Shared SubVS persistence using the API.
PD-7465	Fixed an issue with the DisablePasswordForm API parameter.
PD-7379	Fixed an issue which was preventing the Require SNI hostname flag from being set using the RESTful API.
PD-7267	The Java API ModSSODomain command accepts Map<String, String> as a third parameter.
PD-7192	Fixed a typo in the nameserver API parameter.
PD-7420	The checkheader API parameter now allows the correct number of header/field pairs (up to four).

PD-6923	Fixed the API command to enable/disable SubVSs.
PD-6866	The InputAuthMode API parameter has additional values, as needed.
PD-6865	The CheckHeaders parameter has been added to the modify Virtual Service command.

16.4 Known Issues

PD-11023	A critical vulnerability in the LoadMaster Operating System (LMOS) related to Session Management could allow an unauthorized, remote attacker to bypass security protections, gain system privileges, and execute elevated commands such as **ls**, **ps**, **cat**, and so on, thereby compromising the system. Through this remote execution, in certain cases, exposure of sensitive system data such as certificates, private keys, and other information may be possible. Further information can be found here: Mitigation For Remote Access Execution Vulnerability.
PD-8725	**Proximity** and **Location Based** scheduling do not work with IPv6 source addresses.
PD-9950	LoadMaster VNF HA does not work on LoadMaster versions 7.1.35.*n* and 7.2.36.*n*. It does work om LoadMaster version 7.2.37 and above.
PD-10159	CPU and network usage graphs not appearing after firmware upgrade. Resetting the statistic counters does not clear the graph data.
PD-7218	WAF-FLE servers are not accepting LoadMaster remote logging requests. This is an issue with WAF-FLE rather than the LoadMaster.
PD-7713	There is an issue which is causing the health check status to show as unchecked on Azure HA units, even though the health check probe is working correctly.
PD-7678	There is an issue which is continually locking out some LoadMaster users when using HA and session management. This is because the list of blocked logins is shared between HA machines. When a user is unblocked, the “blocked login” file is

	not removed from both machines – so the files come back from the slave unit. As a workaround – unblock the user on both machines at the same time.
PD-7578	There is an issue where wildcard UDP Virtual Services are not NATing the return traffic as expected.
PD-7265	When the Shared IP Address is changed in a HA pair, the user is not redirected to the new Shared IP Address.
PD-7764	There is an issue which is preventing the ciphers from being selected in the Microsoft Edge and Internet Explorer browsers.
PD-7487	When adding a local user and the name of the user is bal, the response is correct but the response stat is invalid – it should be 400/422 or another stat, but not 200.
PD-7752	RADIUS challenge is sending mangled characters.
PD-7157	There is an issue with using file attachments in SharePoint when using WAF and KCD.
PD-7559	It is not possible to add a comment to a block or whitelist entry using the API.
PD-7556	The PowerShell configure Virtual Service command does not support the ability to set the Persistence Mode to none.
PD-7658	It is not possible to unset any syslog values using the related PowerShell API command.
PD-7657	It is not possible to unset the netconsole parameter using the Set-LmDebugConfiguration command.
PD-7656	It is not possible to unset certain values using the Set-SecRemoteAccess PowerShell API command.
PD-7655	The bonded interface API commands are returning errors.
PD-7650	There are some issues relating to the setwafautoupdate API command.
PD-7648	It is not possible to upload a custom rule data file to the LoadMaster using the RESTful API.
PD-7643	Manual reboots using the API do not reset the reboot counter, which can cause the LoadMaster to enter passive mode after rebooting three times without the LoadMaster being up for more

	than five minutes.
PD-7608	It is not possible to enable the “Require SNI hostname” flag using the modify Virtual Service PowerShell and Java API commands.
PD-7693	When setting the CheckPattern parameter using the API, inputs over 140 characters are being lost and part of the input is spilling over into the CheckHost parameter.
PD-7753	When using the PowerShell API for a LoadMaster with a management port other than 443, you need to specify the port when using the commands Enable-SecAPIAccess and Disable-SecAPIAccess.
PD-7565	The checker address cannot be set using the API.
PD-7522	If a GEO map is modified using the API and the IP address for the site is not specified, nothing is returned (an error should be displayed).
PD-7516	The GEO Location Based option for “Everywhere” cannot be set and is not listed in the API.
PD-7338	The listclusters API command returns 0 as the CheckerPort value if the checker is set to tcp. The default value when using TCP health checks is 80 and that should be returned.
PD-7742	The API and UI allow different lengths for the field DNS query.
PD-7696	The Checked Port cannot be unset using the API.
PD-10160	The API commands to reset the CPU and network graphs do not work.

17 Release 7.1.34.1

Refer to the sections below for details about firmware version 7.1.34.1. This was released on 18th May 2016.

As of 7.1.34.1, the VMware vCenter Operations (vCOPs) v5 LoadMaster plugin is no longer being maintained because VMware have ended their support of vCOPs v.5.8.1.

Upgrading an existing LoadMaster for Amazon Web Services (AWS) from a pre-7.1.34 firmware version to 7.1.34 and above will not work. This issue is caused by AWS de-emphasizing and eventually deprecating support for Para Virtual (PV) images. Therefore, all new LoadMaster versions will support Hardware Virtual Machine (HVM) AMIs only. For help upgrading please contact KEMP Technical Support.

17.1 New Features

- Improvements made to the home page of the LoadMaster Web User Interface (WUI)
- Template creation capabilities have been added
- Domain Name System Security Extensions (DNSSEC) client support has been added
- Microsoft Azure Resource Manager (ARM) deployment is supported
- The LoadMaster for Amazon Web Services (AWS) supports Bring Your Own License (BYOL)
- Support has been added for RADIUS challenge/response

17.2 Feature Enhancements

- Enhanced the “Permitted Groups” functionality in the Edge Security Pack (ESP) to work with client certificates.
- RSA-SecurID and LDAP dual factor authentication is supported.
- Two Virtual Service application configuration templates have been published:

  a) Dell Wyse vWorkspace

  b) Adobe Connect

- It is possible to configure “non-standard” web server responses as healthy.

- Improvements made to Common Access Card (CAC) WUI authentication.
- Central SSL cipher set management has been added to the WUI and API.
- It is possible to delete custom GEO locations.
- Improved Virtual Service WAF statistics to better reflect WAF health.
- When SSOMGR debug traces are enabled, the SSOMGR log file gets compressed at midnight, as long as the file is not empty.
- It is possible to license the LoadMaster using a HTTP(S) proxy during installation.
- Added support for virtIO disks for KVM LoadMasters.
- Extended region support has been added for LoadMasters in AWS.
- Added a new L7 configuration option which allows empty headers.
- Added a PowerShell API command to add a SubVS.
- Added a parameter for Subnet Originating Requests to the Virtual Service API commands.
- Added PowerShell API commands relating to health check aggregation and configurable health thresholds.
- PowerShell and Java API commands have been added for adding custom locations to FQDNs.
- Improvements made to the PowerShell API in relation to Virtual Services and SubVSs.
- Replaced the API parameters **tcpfailover** and **cookieupdate** with **hal4update** and **hal7update**, respectively.
- Updated OpenSSL to version 1.0.2h to mitigate against the CVE-2016-2107 vulnerability.
- Mitigated against CVE-2015-5621 vulnerability.

17.3 Issues Resolved

PD-7035	Increased the length of the redirect URL field.
PD-6644	Changed the VLAN interface ID to the actual VLAN number.
PD-6921	LDAPS is capable of running in FIPS mode.
PD-6570	Improved WAF stability.
PD-7083	Improved RADIUS health checks.
PD-7064	Fixed an issue relating to content rule removal.

PD-6950	Fixed an issue which was causing the administrative certificate to be lost after reboot.
PD-6936	Fixed a license error which was occurring after certain upgrades.
PD-6931	Fixed the historical statistics page on nodes in a cluster.
PD-6916	Fully removed support for SSHv1.
PD-6870	Improved failed login attempt threshold enforcement.
PD-6653	Improvements made to the WAF counter on the home page.
PD-6656	It is possible to manipulate the host file from the LoadMaster by specifying the IP address and host FQDN for the entry.
PD-6468	Improved WAF performance.
PD-6412	Enhanced support for multi-domain forests within ESP.
PD-4666	Fixed error in SSO configuration logs regarding lost domain.
PD-7222	Enhanced WAF syslog support.
PD-6591	Improved Kerberos Constrained Delegation (KCD) service ticket handling.
PD-6549	Fixed an issue with deleting VLAN/VXLANs when in High Availability (HA) mode.
PD-6731	Fixed an issue which was causing the Real Server status to not display correctly when Enhanced Options was enabled.
PD-6657	Fixed an issue relating to Private/Public site preference with Proximity scheduling.
PD-6641	Fixed a display issue for sites using a built-in geographic location database.
PD-6626	Fixed geographic coordinate resolution of existing sites when switching to proximity selection.
PD-6607	Fixed an issue when using KCD OWA and file attachments with SharePoint and Exchange.
PD-6760	Enhanced the POST health check to handle special characters in the POSTDATA.
PD-6734	Improved synchronization with SharePoint One Drive when using ESP form-based authentication and KCD.

PD-6669	Fixed an issue with legacy licensing on the free Virtual LoadMaster.
PD-6548	Resolved an issue which was causing high CPU usage when additional services were added.
PD-6459	Fixed incorrect CPU statistics.
PD-6329	Added missing Java and PowerShell API commands relating to the Packet Routing Filter.
PD-6215	Added API commands to allow public IP addresses to be treated as private on GEO.
PD-6214	Added an API command to limit the number of concurrent logon sessions.
PD-6617	Added an API command which lists all installed certificates.
PD-6864	Added a parameter for Quality of Service to the API.
PD-6958	The System Center plugin can reach the LoadMaster API.
PD-6928	Fixed an issue with the API command to enable non-local Real Servers.
PD-6365	Added a missing PowerShell API parameter value for “Username only” in the Set-SSODomain command.
PD-7067	Added an API parameter to set Basic Authentication.
PD-7049	Improved error handling for the ErrorUrl RESTful API parameter.
PD-7020	Fixed an API issue relating to using the Transparent parameter with the Sorry Server parameter.
PD-6978	Added the RSIndex parameter to the PowerShell and Java API.
PD-6860	Fixed error handling in the API for the alternate address parameter.
PD-6841	The API correctly reflects the Virtual Service status.
PD-6602	Fixed the API response for the command to get the administrative certificate.
PD-6600	Improved an API display issue relating to the MatchRules section of Real Server output.
PD-6595	Improved error handling when disabling ACLControl using the API.
PD-6481	Fixed an API issue in the LoadMaster for Azure when adding/modifying Virtual Services.

PD-6213	Cipher set management added to the Java API.
PD-6195	Added PowerShell and Java API commands relating to managing the black and white list.
PD-6846	Added the VSIndex parameter to the Set-VirtualService command in the PowerShell API.
PD-6843	Fixed an issue with the Get-NetworkOptions PowerShell API command.
PD-6655	Improved error handling for the API list commands.
PD-6601	Improved the HTTP status code in the RESTful API command to set the local cert.
PD-6599	Improved the GetSDNController Java API command.
PD-6598	Improved the AddSDNController and ModSDNController Java API commands.
PD-6587	Fixed the response of the New-RealServer PowerShell API command.
PD-6480	Improved the PowerShell API command Set_AWSHAOption.
PD-7647	Fixed an issue which was causing WUI connection problems on LoadMasters for Azure. Please update the Azure add-on in addition to the LoadMaster firmware to fix this issue.

17.4 Known Issues

PD-11023	A critical vulnerability in the LoadMaster Operating System (LMOS) related to Session Management could allow an unauthorized, remote attacker to bypass security protections, gain system privileges, and execute elevated commands such as **ls**, **ps**, **cat**, and so on, thereby compromising the system. Through this remote execution, in certain cases, exposure of sensitive system data such as certificates, private keys, and other information may be possible. Further information can be found here: Mitigation For Remote Access Execution Vulnerability.
PD-7173	Pre-authorization excluded directories do not work as expected with KCD.
PD-7127	The SSOMGR is not purging the Kerberos cache cleanly.
PD-7099	It is not always possible to create a SubVS within a Log Insight Virtual Service in the LoadMaster WUI.

PD-7157	There is an issue with using file attachments in SharePoint when using WAF and KCD.
PD-7121	OCSP responses containing multiple certificates are not processed correctly.
PD-7056	There is an issue relating to black list IP addresses in Virtual Services.
PD-7047	There is an issue with Name Server (DNS) protocol health checking.
PD-7226	There is an issue uploading some templates which contain long comments.
PD-7023	The output and error handling of the Get-Rule API command is not ideal.
PD-7016	The IncludeQuery API parameter cannot be set.
PD-6930	The IPv6 support in the API is incomplete.
PD-7225	The listcustomlocation API command shows custom locations that have not been added.
PD-7128	The persist parameter does not appear in the API command showvs output when the persistence mode is set to Source IP Address.
PD-7021	There is a discrepancy between the length of the Add Header to Request field between the WUI and API.
PD-7014	There is an issue removing extra ports when using the PowerShell API.

18 Release 7.1-32a

Refer to the sections below for details about firmware version 7.1-32a. This was released on 26th January 2016.

18.1 New Features

- A HTTP/2 Virtual Service type has been added
- High Availability (HA) in the LoadMaster for Amazon Web Services (AWS)
- LoadMaster Clustering
- Health check aggregation and threshold configuration
- A WAF event log has been added.
- Remote WAF logging functionality has been added.
- Some of the WAF WUI fields have been renamed to increase clarity.
- A WAF rule updates log has been added to increase clarity.
- The WAF audit logs are available using the API and can be sent to third party collectors.

18.2 Feature Enhancements

- Updated the LoadMaster root certificate to mitigate against CVE-2004-2761 vulnerability.
- The PowerShell API library supports only TLS 1.1 and TLS 1.2.
- The Java API supports Java 7 and Java 8.
- API support added for SSH and Web User Interfaces (WUI) pre-authentication messages.
- Multiple NICs are supported in the LoadMaster for Azure.
- Multiple subnets are supported in the LoadMaster for Azure.
- A number of Virtual Service application configuration templates have been published:

    a) AD FS v3

    b) DirectAccess

    c) Fujifilm Synapse

    d) Skype for Business

    e) Greenway PrimeSuite

f) Epicor ERP

g) Microsoft Exchange 2016

- Updates have been made to the Microsoft Exchange 2013 Virtual Service application configuration templates.
- Improvements have been made to the display of the sections on the Modify Virtual Service screen.
- More information has been added to the screen where the license type is selected when initially configuring a LoadMaster.
- Improved VXLAN/VLAN interface usability.
- Warning added to prevent the enabling of cluster mode if VXLANs or IPsec tunnelling is enabled.
- FIPS mode forces the use of Session management mode.
- Authenticated NTPv4 is supported.
- Additional Security headers are included on WUI pages.
- Administrative actions are written in an audit log.
- It is possible to enable pre-authentication click through banner.
- If session management is enabled, the last successful login is displayed on the home page of the LoadMaster WUI.
- When using the Edge Security Pack (ESP), it is possible to steer traffic based on Active Directory group membership.
- Nested permitted groups are supported when using ESP.
- The Cavium driver has been updated to V6.0.

18.3 Issues Resolved

PD-6523	Improved the way the SSL reencrypt parameter is set in the PowerShell API.
PD-6482	Fixed an issue relating to bonded interfaces and the active/backup option.
PD-6476	Improved GEO proximity stability.
PD-6435	Fixed an issue relating to HA and SSO synchronization.
PD-6413	It is possible to use port following with wildcard ports.
PD-6389	Fixed an issue where image set resources did not load if there were no Real Servers present.

PD-6385	Added the ability to select the TLS version for the WUI.
PD-6364	Consistency improvements made between the RESTful, PowerShell and Java APIs.
PD-6348	Improved RADIUS authorization stability.
PD-6334	Fixed an issue relating to WUI access when using FIPS mode and TLS 1.2.
PD-6231	Added some commands that were missing from the PowerShell API.
PD-6167	Fixed an issue relating to SNMP and IPv6.
PD-6165	Fixed a WUI compatibility issue with Internet Explorer 11.
PD-6160	Improved API usability when creating a Virtual Service with SSL reencryption.
PD-6159	Improved WAF and Virtual Service stability.
PD-6096	Improved Azure Virtual LoadMaster (VLM) stability.
PD-6077	Fixed an issue which was causing VLMs to hang in certain scenarios.
PD-6013	It is possible to set Subnet Originating Requests per Virtual Service using the API.
PD-5961	Fixed an issue which was preventing attachments greater than 1MB from being attached when using Kerberos Constrained Delegation.
PD-5932	Fixed an issue which was causing a segfault in some situations.
PD-5915	Fixed an issue which was preventing an extra name server from being added.
PD-5909	Fixed a minor issue relating to the API command used to display the black list.
PD-5857	Fixed an issue which was causing a collector thread error in the VMware vRealize Operations Manager.
PD-5798	Updated firmware to mitigate against CVE-2015-5600 vulnerability.
PD-5641	Fixed an issue which was causing LM-2600 models to reboot when configuration changes were made.
PD-5222	Fixed an issue relating to short domain names.
PD-4775	Fixed an issue which was causing Virtual Services in a Security Down state to be listed as “InService” when querying using SNMP.
PD-3642	Fixed an issue relating to GEO Weighted Round Robin statistics.

PD-6102	Fixed an issue with the enable Real Server button.
PD-6514	Fixed an issue relating to site restrictions for FQDNs.
PD-6095	Fixed an issue with the add/remove country and change map location API commands for GEO.
PD-6078	It is possible to add a custom location to an IP in an FQDN using API commands.
PD-6735	Fixed a synchronization issue when using Kerberos Constrained Delegation (KCD) with SharePoint.
PD-6703	Fixed an error in the SSO configuration logs regarding details being lost for a domain.
PD-6404	Improved error handling for API list commands.

18.4 Known Issues

PD-11023	A critical vulnerability in the LoadMaster Operating System (LMOS) related to Session Management could allow an unauthorized, remote attacker to bypass security protections, gain system privileges, and execute elevated commands such as **ls**, **ps**, **cat**, and so on, thereby compromising the system. Through this remote execution, in certain cases, exposure of sensitive system data such as certificates, private keys, and other information may be possible. Further information can be found here: Mitigation For Remote Access Execution Vulnerability.
PD-6626	Changing an existing FQDN with sites to proximity balancing causes automatic resolution to fail.
PD-6627	If 'bad data' is entered in the coordinates of an FQDN, automatic resolution will fail.
PD-6575	There is an issue which is preventing the OpenStack Load Balancer as a Service (LBaaS) from being installed in some scenarios.
PD-4666	In some cases, SSO configuration details are being lost.
PD-6607	When using WAF and KCD – file attachments fail with SharePoint and Exchange.
PD-6591	In some situations, the LoadMaster is not requesting the KCD service ticket.

19 Release 7.1-30a

Refer to the sections below for details about firmware version 7.1-30a. This was released on 2nd November 2015.

19.1 Feature Enhancements

- API commands have been added to retrieve SDN device and path information.
- Updated firmware to mitigate against CVE-2015-5600 vulnerability.

19.2 Issues Resolved

PD-6335	Fixed an issue relating to using FIPS mode and TLS 1.1 or 1.2.
PD-6223	Fixed an issue which was causing some LM-2600 models to reboot when configuration changes were made.
PD-6222	Fixed an issue which was causing some Virtual LoadMasters to hang.

19.3 7.1-30a - Known Issues

PD-11023	A critical vulnerability in the LoadMaster Operating System (LMOS) related to Session Management could allow an unauthorized, remote attacker to bypass security protections, gain system privileges, and execute elevated commands such as **ls**, **ps**, **cat**, and so on, thereby compromising the system. Through this remote execution, in certain cases, exposure of sensitive system data such as certificates, private keys, and other information may be possible. Further information can be found here: Mitigation For Remote Access Execution Vulnerability.

20 Release 7.1-30

Refer to the sections below for details about firmware version 7.1-30. This was released on 3rd November 2015.

20.1 New Features

- IPsec Tunnelling Feature Extension
- LoadMaster SDN Adaptive
- VMware vRealize Orchestrator Integration.
- Virtual Extensible LAN (VXLAN) network support
- Multi-domain authentication with the Edge Security Pack (ESP)
- Certificate Authentication for WUI access
- TCP Multiplexing

20.2 Feature Enhancements

- Content switching based on request payload is supported.
- The total number of allowed concurrent administrative logon sessions to the LoadMaster WUI is configurable.
- SDN adaptive mode settings can be fully configured using the API.
- SDN-related commands have been added to the PowerShell and Java APIs.
- Script version information has been added to the LoadMaster logs.
- Memory utilization enhancements have been made for Web Application Firewall (WAF).
- Special characters are allowed in Virtual Service names.
- Manual boot options and a hardware compatibility check has been added to the bare metal installation.
- Granular control over cipher sets has been added to SSL certificate management.
- The LoadMaster OpenSSL version has been upgraded to 1.0.1p.
- Short domain names are supported when using ESP.
- The Web User Interface (WUI) has been updated with a new color scheme and improved navigation.
- An Oracle EBS Virtual Service application configuration template has been published.

- An SAP Virtual Service application configuration template has been published.
- An Oracle JD Edwards Virtual Service application configuration template has been published.
- FIPS 140-2 Level 1 operation is available in all LoadMaster models.
- LoadMaster can use a proxy for internet access.
- Diffie-Hellman Exchange (DHE) key size can be specified.
- WUI indicators for High Availability status of Azure-based LoadMasters and GEO has been improved
- The filename of manual LoadMaster backups includes the LoadMaster host name.
- Reply code of 200 has been added to the Not Available Redirection Handling.
- SNMP protocol version and authentication settings are configurable.
- Selective response settings for public or private sites based on request source are more granularly configurable.
- It is possible to flush the SSO cache using the API.
- The Custom Headers field in the Real Server Check Parameters accepts special characters.

20.3 Issues Resolved

PD-5841	Fixed an issue relating to the username when configuring SNMP v3.
PD-5643	Fixed an issue which was causing problems with automated backups.
PD-5500	Fixed an issue relating to permitted groups and ESP authentication.
PD-5420	Fixed an issue which prevented the Not Available Redirection Handling Error File from being updated.
PD-5416	Fixed an issue relating to RSA authentication prompts.
PD-4964	Fixed an issue relating to RSA concurrent access.
PD-4596	Fixed an issue where the LoadMaster was not sending full certificate data on the front-end handshake.
PD-3726	Fixed an issue which was causing the LoadMaster to reboot on KCD login.
PD-4865	Fixed an issue relating to unlocking locked users for some SSO domains.
PD-5920	Fixed an issue which was showing RS health check status as “up” even when it was unavailable.
PD-5870	Fixed an issue which was preventing logs from appearing in Internet Explorer.

PD-5867	Fixed an issue relating to two-factor (RADIUS and LDAP) ESP authentication.
PD-5853	Fixed an issue relating to GEO health checking.
PD-5586	Fixed an issue where toggling scheduling methods was causing the LoadMaster to crash.
PD-5282	Fixed an issue relating to the GEO proximity scheduling method.
PD-4863	Fixed an issue which was preventing GEO custom locations from being edited.
PD-5478	Fixed an issue with the GEO round robin scheduling method for IPv6.
PD-4662	Fixed an issue which was causing the LDAP health check to fail intermittently.
PD-3567	Fixed an issue relating to gratuitous ARP on IPv4 when using IPv6 and additional addresses.
PD-5863	Fixed Network Interface Card (NIC) port mapping for 8-NIC LoadMaster units.

20.4 Known Issues

PD-11023	A critical vulnerability in the LoadMaster Operating System (LMOS) related to Session Management could allow an unauthorized, remote attacker to bypass security protections, gain system privileges, and execute elevated commands such as **ls**, **ps**, **cat**, and so on, thereby compromising the system. Through this remote execution, in certain cases, exposure of sensitive system data such as certificates, private keys, and other information may be possible. Further information can be found here: Mitigation For Remote Access Execution Vulnerability.
PD-5582	There are some GEO issues relating to the resource check parameters and cluster health checking.
PD-4666	In some cases, SSO configuration details are being lost.
PD-5915	In GEO, it is not possible to add multiple name servers using the WUI. This can be done in the API as a workaround.
PD-5909	The RESTful API stops displaying blacklist IP addresses after 325 entries.
PD-5641	In certain situations, LM-2600 LoadMasters are rebooting when configuration changes are made.
PD-5857	There are issues with the VMware vRealize Operations collector for the

	LoadMaster.
PD-5961	Attachments greater than 1MB will not work if the authentication mode is set to Kerberos Constrained Delegation (KCD).
PD-6102	The enable Real Server button is not functioning correctly.

21 Release 7.1-28b

Refer to the sections below for details about firmware version 7.1-28b. This was released on 28th August 2015.

21.1 Feature Enhancements

- A new reply code of **200 OK** has been added to the **Not Available Redirection Handling Error Code** drop-down list.
- Updated firmware to mitigate against CVE-2015-5477 vulnerability.

21.2 Issues Resolved

PD-5596	Fixed an issue which prevented the Not Available Redirection Handling error file from being updated.
PD-5581	Fixed a GEO Web User Interface (WUI) issue which caused issues with multiple locations being assigned.
PD-5513	Improvements have been made to increase LoadMaster stability.

21.3 Known Issues

PD-11023	A critical vulnerability in the LoadMaster Operating System (LMOS) related to Session Management could allow an unauthorized, remote attacker to bypass security protections, gain system privileges, and execute elevated commands such as **ls**, **ps**, **cat**, and so on, thereby compromising the system. Through this remote execution, in certain cases, exposure of sensitive system data such as certificates, private keys, and other information may be possible. Further information can be found here: Mitigation For Remote Access Execution Vulnerability.
PD-3567	No gratuitous ARP is sent on IPv4 when using IPv6 and additional addresses.
PD-3642	Statistics are not updating correctly when using GEO and weighted round robin scheduling.
PD-4662	There is an intermittent issue with the LDAP Health check in certain configurations.

PD-4863	Custom locations on the LoadMaster GEO cannot be disabled.
PD-4865	In certain domains, locked users cannot be unlocked.
PD-4964	RSA Authentication fails when the RSA Test User is configured.
PD-5020	The Custom Header field in Real Server Check Parameters does not accept special characters.
PD-5416	ESP RSA does not always require RSA passphrase for new connection if the user has an existing session.
PD-5420	The Error File for Not Available Redirection Handling cannot be updated.

22 Release 7.1-28a

Refer to the sections below for details about firmware version 7.1-28a. This was released on 29th July 2015.

22.1 New Features

- Microsoft SharePoint templates have been created.
- MobileIron templates have been created.

22.2 Feature Enhancements

- Commands relating to SDN have been added to the RESTful API
- Stated Real Server limits are calculated on a per LoadMaster basis.
- The maximum number of concurrent SSL connections scales better with memory.
- Alternate source addresses can be set when SSL re-encryption is enabled.

22.3 Issues Resolved

PD-5413	Fixed an issue relating to the Service Provider License Agreement (SPLA) licensing screen where the online/offline option was sometimes hidden.
PD-4924	Improved stability when using the Edge Security Pack (ESP) **Delegate to Server** option.
PD-4597	Fixed a memory issue relating to nested Virtual Services.
PD-5251	Fixed an issue which prevented some GEO miscellaneous parameters to be set.
PD-4350	Fixed an issue relating to setting the administrative interface and administrative gateway together.

22.4 Known Issues

PD-11023	A critical vulnerability in the LoadMaster Operating System (LMOS) related to Session Management could allow an unauthorized, remote attacker to bypass security protections, gain system privileges, and execute elevated commands such as **ls**, **ps**, **cat**, and so on, thereby compromising the system. Through this remote execution, in certain cases, exposure of sensitive system data such as certificates, private keys, and other information may be possible.

	Further information can be found here: Mitigation For Remote Access Execution Vulnerability.
PD-3567	No gratuitous ARP is sent on IPv4 when using IPv6 and additional addresses.
PD-3642	Statistics are not updating correctly when using GEO and weighted round robin scheduling.
PD-4662	There is an intermittent issue with the LDAP Health check in certain configurations
PD-4863	Custom locations on the LoadMaster GEO cannot be disabled
PD-4865	In certain domains, locked users cannot be unlocked
PD-4964	RSA Authentication fails when the RSA Test User is configured
PD-5020	The Custom Header field in Real Server Check Parameters does not accept special characters
PD-5416	ESP RSA does not always require RSA passphrase for new connection if the user has an existing session.
PD-5420	The Error File for Not Available Redirection Handling cannot be updated

23 Release 7.1-28

Refer to the sections below for details about firmware version 7.1-28. This was released on 24th June 2015.

23.1 New Features

- ESP enhancement - Dual Factor Authentication
- LoadMaster Clustering - Beta
- ESP enhancement - NTLM support - Beta
- SNMP v3

23.2 Feature Enhancements

- Updated the bare metal installation process.
- Updated the SDN Add-on pack to support Mode 2.
- ESP has a configurable timeout option for SSO forms.
- Further strengthened WUI security.
- Improved the usability of the Session Management function.
- Commands relating to Content Switching have been added to the RESTful API
- Commands relating to changing the Admin Gateway and the Interface have been added to the RESTful API
- Commands relating to Client IP support have been added to the RESTful API
- Commands relating to SDN-Adaptive have been added to the RESTful API
- Commands relating to the Logon Transcode option have been added to the PowerShell and Java APIs
- Improved the syslog with multiple destinations.
- Improved the display of the state of add-on packs in the WUI.
- Added notifications for when Virtual Service Connection Limits are reached.
- Improved ESP logging to show which URLs are being accessed by users.
- Increased the size of the Match field in Content Rules.
- Improved the backup function by including SSO images.

- Improved the initial setup process of AWS.
- Added support for VMware Log Insight 2.5.
- Improved pre-licensing troubleshooting.
- Improved logon format for Dual Factor Authentication.
- Increased the maximum length of the RADIUS Shared Secret.
- Improved the security around the RADIUS Shared Secret.
- Improved the new software availability alert functionality.
- Added new diagnostic tools.
- Improved Java API error handling
- Added SubVS status to the output of the Showvs RESTful API command
- Improved the handling of SAN certificates on AWS

23.3 Issues Resolved

PD-4195	Vulnerability - XSS Credited to – Francesco Perna (CVE submitted)
PD-4196	Vulnerability - XSRF Credited to – Francesco Perna (CVE submitted)
PD-4198	Vulnerability - OS Command Injection Credited to – Francesco Perna (CVE submitted)
PD-4199	Vulnerability - Cross Site Scripting Injection Credited to – Roberto Suggi Liverani and Paul Heneghan (CVE submitted)
PD-1677	Gave path to RESTful API command for uploading node secret and config file of RSA settings

PD-3697	Fixed issue with ESP SMTP
PD-4212	Fixed header injection issue with X-Forwarded_For
PD-4305	Improved RESTful API return code for listvs command
PD-4383	Fixed issue with subnet originating and re-encrypt
PD-4385	Improved SSO Manager stability
PD-4519	Fixed issue for WUI refresh with adaptive agent
PD-4528	Fixed issue with input error handling for IPSec configuration
PD-4529	Fixed issue with Java API relating to SetParameter() method
PD-4531	Fixed issue with LM default gateway after VS IP change
PD-4534	Fixed issue with IPv6 healthcheck
PD-4535	Fixed issue with intermediate certificates display
PD-4542	Fixed FIPS Reencrypt SSL
PD-4543	Fixed FIPS Reverse SSL
PD-4559	Fixed issue in PowerShell API for SNMP option
PD-4604	Fixed issue where a user may lose access to diagnostic shell
PD-4608	Fixed issue where changing global default gateway causes WUI admin to lose access
PD-4629	Fixed SDN view logs selection issue
PD-4648	Fixed issue with custom image sets relating to long image file name
PD-4663	Improved error handling for SDN controller inputs
PD-4693	Fixed issue with SDN Adaptive scheduling
PD-4704	Fixed issue with special characters in PSK for IPSec configuration
PD-4710	Fixed RESTful API command for modrs relating to IPv6
PD-4712	Fixed issue with removal of certificates in relation to other VS
PD-4802	Fixed SDN display on WUI
PD-4828	Improved security in backup
PD-4855	Improved SDN security

PD-4884	Fixed issue with GEO partners and HA
PD-4917	Fixed issue with home page graphs on 32bit systems
PD-4954	Fixed issue with statistics showing adaptive value for RS
PD-4969	Fixed issue with adaptive agent creating templates
PD-5022	Improved WAF rules installation efficiency
PD-5062	Improved security in SSO manager logs
PD-5119	Improved stability for SSO manager
PD-3703	Fixed an issue relating to the domain\username format when the Logon Format is set to Username in an SSO domain.
PD-4632	Fixed issues relating to the SDN logs date picker.
PD-5124	Fixed an issue relating to persistence and SubVSes.

23.4 Known Issues

PD-11023	A critical vulnerability in the LoadMaster Operating System (LMOS) related to Session Management could allow an unauthorized, remote attacker to bypass security protections, gain system privileges, and execute elevated commands such as **ls**, **ps**, **cat**, and so on, thereby compromising the system. Through this remote execution, in certain cases, exposure of sensitive system data such as certificates, private keys, and other information may be possible. Further information can be found here: Mitigation For Remote Access Execution Vulnerability.
PD-3324	In some situations, R320s are not failing over correctly.
PD-3567	No gratuitous ARP is sent on IPv4 when using IPv6 and additional addresses.
PD-3642	Statistics are not updating correctly when using GEO and weighted round robin scheduling.
PD-5251	Some of the fields on the GEO **Miscellaneous Params** screen cannot be set using the WUI. Most of these fields can be set using the API as a workaround.
PD-4350	There is an issue with setting some RADIUS fields in the WUI in some scenarios.

24 Release 7.1-26c

Refer to the sections below for details about firmware version 7.1-26c. This was released on 20th May 2015.

24.1 Issues Resolved

PD-4666	Fixed an issue relating to the Single Sign On (SSO) domain configuration
PD-4916	Fixes implemented which enhance the IRQ balancing for LoadMaster appliances

24.2 7.1-26c - Known Issues

PD-11023	A critical vulnerability in the LoadMaster Operating System (LMOS) related to Session Management could allow an unauthorized, remote attacker to bypass security protections, gain system privileges, and execute elevated commands such as **ls**, **ps**, **cat**, and so on, thereby compromising the system. Through this remote execution, in certain cases, exposure of sensitive system data such as certificates, private keys, and other information may be possible. Further information can be found here: Mitigation For Remote Access Execution Vulnerability.

25 Release 7.1-26

Refer to the sections below for details about firmware version 7.1-26. This was released on 1st May 2015.

25.1 New Features

- A Moodle template has been released
- A VMware View 6 template has been released
- Qualified IPsec tunnelling with Microsoft SharePoint
- Enhancements made to the Software Defined Networking (SDN) adaptive add-on pack

25.2 Feature Enhancements

- Fixed an issue relating to Kerberos Constrained Delegation (KCD) working with the Web Application Firewall (WAF)
- Updated the copyright on the LoadMaster console and WUI screens.
- Added logging for Edge Security Pack (ESP) permitted group failures.
- Added an option to send SNMP traps form the shared IP address when in HA mode.
- Commands relating to add-ons have been added to the Java and PowerShell APIs.
- Commands relating to licensing have been added to the RESTful, PowerShell and Java APIs.
- IPsec tunnelling support has been added to the Application Program Interfaces (APIs)
- User management support has been added to the APIs
- Additional statistics support has been added to the APIs
- Expansion of RESTful API permissions
- Improvements made to the ping debug option.
- POST health check character limit increased
- Improved session management security
- Improved security on the Web User Interface (WUI)
- Improved security relating to cross-site request forgery
- Updated firmware to mitigate against CVE-2015-0204, CVE-2015-0286, CVE-2015-0287, CVE-2015-0289, CVE-2015-0293, CVE-2015-0209 and CVE-2015-0288 vulnerabilities

25.3 Issues Resolved

PD-4285	Removed an invalid option (Port Following) from the SubVS screen.
PD-4188	Improved Virtual Service statistic reporting.
PD-4071	Fixed an issue which caused some connections to time out in certain scenarios.
PD-3985	Improved security relating to ActiveSync logins.
PD-3910	Fixed an issue which prevented temporary licenses from being applied to hardware LoadMasters.
PD-3774	Fixed an issue with DNS health checking.
PD-3681	Fixed an issue relating to the HTTP transfer encoding reaching the maximum character limit.
PD-3567	Improved High Availability (HA) failover with IPv6.
PD-4118	It is possible to import a certificate with a separate key file.
PD-4212	Fixed an issue relating to X-Forwarded-For header injection.
PD-4169	Fixed an issue relating to Real Server persistence.
PD-4117	Fixed an issue which caused the LoadMaster to lock up in certain scenarios.
PD-4061	Fixed an issue relating to Active Cookie persistence.
PD-3610	Fixed an issue which caused the LoadMaster to reboot unexpectedly in certain scenarios.
PD-4481	Fixed an issue which caused a LoadMaster HA unit to stop responding in a certain scenario.
PD-3780	Vulnerability - Denial of Service Condition Credited to – Roberto Suggi Liverani and Paul Heneghan (CVE submitted)
PD-3781	Vulnerability - Cross Site Request Forgery Credited to – Roberto Suggi Liverani and Paul Heneghan (CVE submitted)

PD-4484	Fixed an issue which was causing the LoadMaster installation to fail on Fujitsu bare metal platforms.

25.4 Known Issues

PD-11023	A critical vulnerability in the LoadMaster Operating System (LMOS) related to Session Management could allow an unauthorized, remote attacker to bypass security protections, gain system privileges, and execute elevated commands such as **ls**, **ps**, **cat**, and so on, thereby compromising the system. Through this remote execution, in certain cases, exposure of sensitive system data such as certificates, private keys, and other information may be possible. Further information can be found here: Mitigation For Remote Access Execution Vulnerability.
PD-3324	In some situations, R320s are not failing over correctly.
PD-3567	No gratuitous ARP is sent on IPv4 when using IPv6 and additional addresses.
PD-3682	Virtual Service statistic details are incorrect in some situations.
PD-3642	Statistics are not updating correctly when using GEO and weighted round robin scheduling.
PD-3703	In some situations, the domain\username format is not working when the Logon Format is set to Username in an SSO domain.
PD-4383	Per-SubVS Subnet Originating Requests are not working when using reencryption.
PD-4516	Centaur processors are not supported.
PD-4531	The LoadMaster is ignoring the per-service default gateway after the virtual IP address is changed.
PD-4648	Images with long filenames are not working in custom SSO image sets.
PD-4608	In certain scenarios, changing the global default gateway causes the WUI to become inaccessible.
PD-4604	The Diagnostic Shell option in the LoadMaster console is inaccessible.

26 Release 7.1-24b

Refer to the sections below for details about firmware version 7.1-24b. This was released on 3rd March 2015.

26.1 New Features

- Free LoadMaster product

26.2 Feature Enhancements

- Updated the version of BIND on the LoadMaster to 9.9.6-P1 to mitigate against the CVE-2014-8500 vulnerability.

26.3 Issues Resolved

PD-4042	Fixed an issue which caused FIPS LoadMasters to lose access to the Web User Interface (WUI) in certain situations.
PD-3911	Fixed an issue which was causing the Web Application Firewall (WAF) to block content when set to **Audit Only** mode.
PD-3330	Fixed an issue which caused the URL to be improperly encoded when using **Form Based** authentication.
PD-3843	Fixed an issue where Web Application Firewall (WAF) rule updates caused the LoadMaster backup file size to increase.

26.4 Known Issues

PD-11023	A critical vulnerability in the LoadMaster Operating System (LMOS) related to Session Management could allow an unauthorized, remote attacker to bypass security protections, gain system privileges, and execute elevated commands such as **ls**, **ps**, **cat**, and so on, thereby compromising the system. Through this remote execution, in certain cases, exposure of sensitive system data such as certificates, private keys, and other information may be possible. Further information can be found here: Mitigation For Remote Access Execution Vulnerability.
PD-3156	Certain Kerberos ticket sizes cause connections to drop.
PD-2586	Virtual IP detail statistics are incorrect.

PD-1677	RSA config and node secret files cannot currently be uploaded to the LoadMaster using the RESTful API.
PD-3681	Some valid regular expressions are causing a syntax error.
PD-3333	Licensing requests can be delayed and can time out in certain scenarios.
PD-4118	Importing a .pem certificate with a separate key file causes a missing key file error. As a workaround, combine the certificate and key into one file (by using the **cat** command) and upload the combined file.

27 Release 7.1-24a

Refer to the sections below for details about firmware version 7.1-24a. This was released on 11th February 2015.

27.1 New Features

- VPN tunneling is supported
- The Log Insight add-on pack is installed on LoadMasters by default.
- The LoadMaster works with SafeNet Hardware Security Module (HSM) devices.
- The LoadMaster FIPS software supports OpenSSL v1.0.1e on the current FIPS card.
- OpenStack support added

27.2 Feature Enhancements

- There is no longer a need to reboot after disabling SSL renegotiation.
- The OpenSSL version on the LoadMaster has been updated to OpenSSL 1.0.1k.
- When an SSL Virtual Service thread limit is reached, the current connection count on all Virtual Services are displayed in the logs.
- The Netstat log includes the listening port, iptables, and NAT information.
- The LoadMaster for Azure shows the external IP address in the console after the setup is completed.
- The RESTful API command to add a Virtual Service has been improved.

27.3 Issues Resolved

PD-3843	Improved the stability of Web Application Firewall (WAF) updates.
PD-3617	Fixed an issue where SubVSs maintained persistence even when they were down.
PD-3530	The LoadMaster supports the download of EC certificates.
PD-3037	Fixed an issue with the LoadMaster for Azure where the HA master unit was not recovering after a failure or reboot.
PD-2859	Fixed an issue which was preventing some HA backups from being restored.
PD-3773	Issues with using the preferred host HA option when WAF is enabled have

	been resolved.
PD-3570	Hostname information has been added to LoadMaster backup files.
PD-3467	Messaging relating to password security strength has been improved.
PD-3404	Fixed an issue which prevented customers with Service Provider License Agreements (SPLA) from accessing the LoadMaster console.
PD-3393	Fixed an issue which prevented Fully Qualified Domain Names (FQDNs) which started with a period (.) from being deleted.
PD-3306	Fixed a routing issue relating to static routes.
PD-3299	Fixed an issue which prevented users with usernames containing a comma (,) from being modified or deleted.
PD-3260	Fixed an issue relating to storage of the home page statistic graphs.
PD-3221	Fixed an issue relating to Edge Security Pack (ESP) passwords containing UTF8 characters.
PD-3220	LoadMaster will continue handling traffic using the default Exchange image set, even when the Portuguese or French Canadian image sets are assigned during an upgrade from 7.1-16 to 7.1-24 or higher.
PD-3187	Fixed an issue relating to the status display of Virtual Services with “redirect” SubVSs.
PD-2992	Fixed an issue relating to CPU temperature statistics display.
PD-3161	Fixed an issue with reverse SSL.
PD-3176	Fixed an issue relating to the **TLStype** RESTful API parameter not being saved.
PD-3160	Fixed an issue with the **modmap** RESTful API command.
PD-3106	The Virtual Service status is updated correctly in the RESTful API when a Real Server is disabled.
PD-3104	The **addmap** RESTful API command works in all scenarios.
PD-3075	A superfluous error message, which displayed when setting the **isolateips** parameter using the **ModifyFQDN** command, has been removed.

27.4 Known Issues

PD-11023	A critical vulnerability in the LoadMaster Operating System (LMOS) related to Session Management could allow an unauthorized, remote attacker to bypass security protections, gain system privileges, and execute elevated commands such as **ls**, **ps**, **cat**, and so on, thereby compromising the system. Through this remote execution, in certain cases, exposure of sensitive system data such as certificates, private keys, and other information may be possible. Further information can be found here: Mitigation For Remote Access Execution Vulnerability.
PD-4042	In certain situations, upgrading a FIPS LoadMaster from version 7.0-10 to 7.1-24a causes the WUI to become inaccessible. This issue does not occur when installing 7.1-24a from an ISO image.
PD-3156	Certain Kerberos ticket sizes cause connections to drop.
PD-2586	Virtual IP detail statistics are incorrect.
PD-1677	You cannot currently upload RSA config and node secret files to the LoadMaster using the RESTful API. However, it is possible using the WUI.
PD-3681	Some valid regular expressions are causing a syntax error.
PD-3333	Licensing requests can be delayed and can time out in certain scenarios.
PD-3330	There is an issue relating to ESP and special characters in a URL.

28 Release 7.1-22b

Refer to the sections below for details about firmware version 7.1-22b. This was released on 3rd December 2015.

28.1 Feature Enhancements

- Improved logs for SSL thread limit.

28.2 Issues Resolved

PD-3287	Fixed an issue with drain time where connections were being dropped without waiting for the drain time.
PD-3338	Improved security on formatted Uniform Resource Identifiers (URI) attacks.
PD-3051	Fixed an issue relating to routing and Server NAT when the packet filter is enabled.
PD-2751	Issues with ActiveSync working with Exchange 2013 have been resolved.
PD-3349	Issues relating to 4K SSL keys which caused some HTTPS Virtual Services to go offline have been resolved.

28.3 Known Issues

PD-11023	A critical vulnerability in the LoadMaster Operating System (LMOS) related to Session Management could allow an unauthorized, remote attacker to bypass security protections, gain system privileges, and execute elevated commands such as **ls**, **ps**, **cat**, and so on, thereby compromising the system. Through this remote execution, in certain cases, exposure of sensitive system data such as certificates, private keys, and other information may be possible. Further information can be found here: Mitigation For Remote Access Execution Vulnerability.
PD-2182	When **Permitted Groups** are set for ESP, users receive an incorrect credential prompt at the forms-based login when the LoadMaster contacts child domains for user authentication.
PD-2586	Virtual IP detail statistics are incorrect.
PD-221	Access to the LoadMaster WUI using an iPhone is not supported.
PD-3161	Reverse SSL does not work correctly.

PD-3160	There is a bug with the **modmap** RESTful API command.
PD-3106	The Virtual Service status is not updated in the RESTful API when a Real Server is disabled.
PD-3104	The **addmap** RESTful API command does not work when the **Selection Criteria** is set to **Real Server Load**.
PD-3075	A superfluous error message appears when you attempt to set the **isolateips** parameter using the PowerShell **ModifyFQDN** command.
PD-2992	The temperature on the **Statistics** screen only shows details for one CPU.
PD-2893	It is possible to upload the same template again in the LoadMaster WUI.
PD-1677	You cannot currently upload RSA config and node secret files to the LoadMaster using the RESTful API. However, it is possible using the WUI.

29 Release 7.1-22

Refer to the sections below for details about firmware version 7.1-22. This was released on 25th November 2014.

29.1 New Features

- Web Application Firewall (WAF)
- New templates
- Web Application Firewall (WAF) API commands
- Template import using API
- New health check
- New Azure billing options
- Akamai add-on pack

29.2 Feature Enhancements

- The layout of the manage SSO domain screen has been improved.
- Virtual Service and Real Server status is available using API commands.
- Updated the time zone data for Russia.
- Add-ons are named based on the LoadMaster version they were made with.
- Cloud-based Virtual LoadMasters have a Web User Interface (WUI) certificate that matches their given FQDN.
- When blocking users - different logon styles for the same username are treated as the same user.
- Arbitrary WUI ports can be set using the Java API.
- Security enhancements have been made to GEO.
- Multiple Virtual Services with the same IP address can be added to the GEO Real Server Load Cluster Check.
- Updated the BIND version to 9.9.6-ESV to address CVE-1999-0662.

29.3 Issues Resolved

PD-2930	Fixed an issue with the "Always check persist" option.
PD-2786	Fixed an issue where ESP logs could not be cleared.
PD-2750	Fixed an issue where creating/editing a Layer 4 Virtual Service would cause connections to drop.
PD-2719	Fixed memory issues on units with bonded interfaces.
PD-2707	Stopped the LoadMaster from mangling UDP packets with a 0 checksum.
PD-3086	Fixed an issue with "Use Address for Server NAT" and SubVSs.
PD-2767	Allowed groups can use the principal name format to log in.
PD-2557	RADIUS authentication should work with Microsoft (and other vendor-based) RADIUS servers.
PD-3023	Fixed an issue with persistence and cookies.
PD-2656	The RESTful API **aclcontrol** command uses correct user permissions.
PD-2574	Issues (relating to ESP and ActiveSync) which were caused by passwords containing non-ASCII characters have been resolved.
PD-2756	A number of GEO bugs have been fixed, for example GEO listens on the specified additional addresses when the **Use for GEO** option is enabled on the interface.
PD-3199	Steps taken to mitigate the following security risk – CVE-2014-3566 ("POODLE")

29.4 Known Issues

PD-11023	A critical vulnerability in the LoadMaster Operating System (LMOS) related to Session Management could allow an unauthorized, remote attacker to bypass security protections, gain system privileges, and execute elevated commands such as **ls**, **ps**, **cat**, and so on, thereby compromising the system. Through this remote execution, in certain cases, exposure of sensitive system data such as certificates, private keys, and other information may be possible. Further information can be found here: Mitigation For Remote Access Execution Vulnerability.

PD-2182	When **Permitted Groups** are set for ESP, users receive an incorrect credential prompt at the forms-based login when the LoadMaster contacts child domains for user authentication.
PD-2586	Virtual IP detail statistics are incorrect.
PD-221	Access to the LoadMaster WUI using an iPhone is not supported.
PD-2751	When using ActiveSync with form-based authentication, occasionally SSO domain connections are dropped.
PD-3161	Reverse SSL does not work correctly.
PD-3160	There is a bug with the **modmap** RESTful API command.
PD-3106	The Virtual Service status is not updated in the RESTful API when a Real Server is disabled.
PD-3104	The **addmap** RESTful API command does not work when the **Selection Criteria** is set to **Real Server Load**.
PD-3075	A superfluous error message appears when you attempt to set the **isolateips** parameter using the PowerShell **ModifyFQDN** command.
PD-2992	The temperature on the **Statistics** screen only shows details for one CPU.
PD-2893	It is possible to upload the same template again in the LoadMaster WUI.
PD-1677	You cannot currently upload RSA config and node secret files to the LoadMaster using the RESTful API. However, it is possible using the WUI.

30 Release 7.1-20d

30.1 Feature Enhancements

- Changes made to allow the Virtual LoadMaster for Azure to be included in the Microsoft Gallery.
- Updates to firmware to mitigate the Shellshock vulnerability.

30.2 Known Issues

PD-11023	A critical vulnerability in the LoadMaster Operating System (LMOS) related to Session Management could allow an unauthorized, remote attacker to bypass security protections, gain system privileges, and execute elevated commands such as **ls**, **ps**, **cat**, and so on, thereby compromising the system. Through this remote execution, in certain cases, exposure of sensitive system data such as certificates, private keys, and other information may be possible. Further information can be found here: Mitigation For Remote Access Execution Vulnerability.
PD-2182	When **Permitted Groups** are set for ESP, users receive an incorrect credential prompt at the forms-based login when the LoadMaster contacts child domains for user authentication.
PD-2586	Virtual IP detail statistics are incorrect.
PD-2656	The RESTful API **aclcontrol** command does not have proper user permissions.
PD-221	Access to the LoadMaster WUI using an iPhone is not supported.
PD-2574	Issues with ESP and ActiveSync if the password contains certain non-ASCII characters.
PD-2751	When using ActiveSync with form-based authentication, occasionally SSO domain connections are dropped.
PD-2750	Occasionally some active Layer 4 Virtual Service connections are dropped when another Layer 4 Virtual Service is created or modified.

31 Release 7.1-20a

31.1 New Features

- New add-on pack to integrate the LoadMaster with VMware vCenter Log Insight.
- New templates to leverage the new Log Insight add-on.
- Support for a new bare metal platform: Fujitsu Primergy.
- Support for Kerberos Constrained Delegation (KCD)
- The ability to designate GEO listening interfaces.
- The ability to use multiple interfaces to listen for GEO requests.
- GEO API commands have been added.
- Web Application Firewall (WAF) – beta release.

31.2 Feature Enhancements

- The OpenSSL version has been upgraded to 1.0.1i.
- The strength of DHE exchange keys for SSL/TLS has been increased.
- A new **Domain/Realm** field has been added to the Manage SSO screen.
- The certificate used by the WUI will take the public name used by Azure/AWS.
- Implemented new Azure requirements

31.3 Issues Resolved

PD-2267	Fixed an issue with the LoadMaster logging process which, in some circumstances, may lead to excessive wear of our Solid State Drives (SSDs)
PD-2648	Fixed a memory issue relating to the SSO manager.
PD-2380	Changed the log level of successful backup notifications.
PD-2598	Fixed an issue with permanent ESP cookies and SubVSs.
PD-2559	Fixed an issue where an SSL Virtual Service might crash.
PD-2485	Made the 100-Continue options clearer in the Web User Interface (WUI).
PD-1728	Fixed an issue with terminal service persistence not being set correctly.

PD-1717	Fixed an issue where changing an interface address would cause an additional address to stop working until the LoadMaster was rebooted.
PD-2349	Reworked the re-encrypt Via header to send HTTPS information.
PD-2252	Fixed an issue where non-checked interfaces did not send Gratuitous ARPs.
PD-2341	Fixed an issue where SNMP did not report the correct status for SubVSs.
PD-2466	Fixed an issue where some HA statistic settings would revert to their previous value.
PD-2310	ESP for SMTP can handle Extended SMTP (ESMTP) chunking.
PD-2481	Fixed a memory issue relating to wildcard Virtual Services.
PD-2508	Fixed an issue where ESP groups had access to other Virtual Services with the same domain.
PD-2560	Enhanced the IMAP health check to make it more RFC compliant.
PD-2641	Increased the strength of the WUI SSL ciphers.
PD-2645	Fixed an issue where statistics were not being refreshed at a proper interval.
PD-2544	GEO wildcard FQDNs are editable.
PD-2536	The **Allow Administrative WUI Access** option is working correctly on the HA shared IP address of additional interfaces.
PD-2253	Memory issue relating to the HA active unit has been fixed.
PD-2101	Fixed an issue where Azure LoadMasters were not starting after a reboot.
PD-2707	Fixed an issue where a 0 checksum UDP packet received from a client was blocked.
PD-2887	The Subject Alternative Name (SAN) in the certificate is used as part of authentication.
PD-2897	Memory issues with bonded interfaces have been resolved

31.4 Known Issues

- A critical vulnerability in the LoadMaster Operating System (LMOS) related to Session Management could allow an unauthorized, remote attacker to bypass security protections, gain system privileges, and execute elevated commands such as **ls**, **ps**, **cat**, and so on, thereby compromising the system. Through this remote execution, in certain cases, exposure of sensitive system data such as certificates, private keys, and other information may be possible.

  Further information can be found here: Mitigation For Remote Access Execution Vulnerability.

- When **Permitted Groups** are set for ESP, users receive an incorrect credential prompt at the forms-based login when the LoadMaster contacts child domains for user authentication.
- Virtual IP detail statistics are incorrect.
- The RESTful API **aclcontrol** command does not have proper user permissions.
- Access to the LoadMaster WUI using an iPhone is not supported.
- Issues with ESP and ActiveSync if the password contains certain non-ASCII characters.
- When using ActiveSync with form-based authentication, occasionally SSO domain connections are dropped.
- Occasionally some active Layer 4 Virtual Service connections are dropped when another Layer 4 Virtual Service is created or modified.

32 Release 7.1-18b

32.1 New Features

- VMware vCenter Operations Management Pack released
- Azure High Availability (HA) enhancements

    a) Azure HA mode health check

    b) Azure HA mode remote synchronization

    c) Azure HA mode WUI changes
- New GEO features which allow failover and isolates public/private sites. Also, two GEO selection criteria options have been renamed to more appropriately reflect their functions (**Location Based** has been renamed to **Proximity** and **Regional** has been renamed to **Location Based**).
- Added Hyper-V Tools support
- New Reencryption SNI Hostname option

32.2 Feature Enhancements

- The Exchange 2013 templates have been updated to reflect Exchange 2013 SP1
- The LoadMaster will pass the host header of HTTPS 1.1 health checks as the server name for Server Name Indication (SNI)
- It is possible to enable Web User Interface (WUI) access on multiple interfaces
- Updated firmware to mitigate against CVE-2014-5287 and CVE-2014-5288 vulnerabilities. Credited to – Roberto Suggi Liverani

32.3 Issues Resolved

PD-2270	Fixed an issue with AWS where a reboot was required after licensing
PD-2292	Fixed an issue with L7 transparency and latency on VMware systems
PD-2407	Fixed an issue where certain persistence modes were not selectable in the Web User Interface (WUI)
PD-2421	Stopped the LoadMaster OS from panicking on VMware Workstation
PD-2445	Fixed an issue that would cause a UDP Virtual Service to not work if a TCP Virtual Service existed using the same IP and port combination

PD-2365	Improvements have been made to the LoadMaster for AWS in relation to Amazon's policies
PD-2183	Functions have been added to sanitize input in the WUI to resolve some security issues – fix for CVE-2014-5287 and CVE-2014-5288
PD-2205	Added new allowed HTTP methods to enable Remote Desktop Services on Windows 8.1
PD-2131	Fixed an issue in Layer 7 UDP services which could have caused the LoadMaster to reboot
PD-2120	Resolved some issues with Layer 4 FTP
PD-2082	SSO configuration is included in automatic configuration backups
PD-1939	SSO configuration is included in manual configuration backups
PD-2065	A new ESP option called Use Session or Permanent Cookies was added which must be set to a permanent cookies option for SharePoint to work correctly with ESP
PD-2043	Increased the maximum number of characters in the RESTful API ciphers parameter to 1023
PD-1989	The underscore character is allowed in the Logoff String field in the ESP options
PD-1984	Removed spurious log messages relating to locked users
PD-1972	Fixed an issue where per-Virtual Service subnet originating addressing was not working when SSL re-encryption was enabled
PD-1958	Added the Additional Headers field in scenarios where it should be displayed but was previously hidden
PD-1952	Fixed an issue where adding a space in the Test User Password field for an SSO domain would cause problems for other fields
PD-1936	HTTP POST health checks send complete information to the Real Server
PD-1935	Fixed an issue where a deleted Virtual Service caused spurious messages in the WUI
PD-1932	Fixed an issue where ESP could reject valid requests
PD-1857	Restructured the Exchange templates

PD-1849	Backslashes are allowed in the Test User field for LDAP SSO domains
PD-1941	Removed unnecessary options for GEO cluster synchronization
PD-2309	Fixed an issue where websites behind the LoadMaster were responding slowly when caching and compression was enabled
PD-2275	Increased thread count to improve throughput
PD-2474	For a SubVS, the HTTP/HTTPS decision is based on the parent Virtual Service settings

32.4 Known Issues

- A critical vulnerability in the LoadMaster Operating System (LMOS) related to Session Management could allow an unauthorized, remote attacker to bypass security protections, gain system privileges, and execute elevated commands such as **ls**, **ps**, **cat**, and so on, thereby compromising the system. Through this remote execution, in certain cases, exposure of sensitive system data such as certificates, private keys, and other information may be possible.

  Further information can be found here: Mitigation For Remote Access Execution Vulnerability.

- GEO health check intervals do not match the settings configured
- The RESTful API command to set the SNMP client only supports IP addresses and not host names (the WUI option supports both)
- Editing an IPv4 address will cause IPv6 addresses to stop responding until a reboot
- There is no option using the RESTful API interface to upload a configuration and node secret file for RSA settings (this can be done using the WUI)
- The RESTful API command to set the NTP host does not allow a URL to be set

33 Release 7.1-16b

33.1 New Features

- Support added for Amazon Web Services (AWS)

33.2 Issues Resolved

PD-2123	Remediation for SSL/TLS MITM vulnerability (CVE-2014-0224) – updated OpenSSL version to 1.0.1h

33.3 Known Issues

- A critical vulnerability in the LoadMaster Operating System (LMOS) related to Session Management could allow an unauthorized, remote attacker to bypass security protections, gain system privileges, and execute elevated commands such as **ls**, **ps**, **cat**, and so on, thereby compromising the system. Through this remote execution, in certain cases, exposure of sensitive system data such as certificates, private keys, and other information may be possible.

  Further information can be found here: Mitigation For Remote Access Execution Vulnerability.

- Changing an IPv4 address causes problems with IPv6
- Issues are experienced when polling the LoadMaster with SNMP when the Default Gateway is on a different interface
- Access to the LoadMaster WUI using iPhones is not supported.
- The **Real Servers are Local** option is not working as expected

34 Release 7.1-16

34.1 New Features

- A new subscription-based online licensing model for the LoadMaster has been implemented
- Full support for UDP at Layer 7
- UDP Layer 7 persistence
- The LoadMaster Operating System is running on Linux kernel 3.10.28
- Added the ability to duplicate a Virtual Service which has SubVSs

34.2 Feature Enhancements

- Added the ability to use a semi-colon in the **SNMP Location** text box
- When ESP is not enabled on any Virtual Service for a particular SSO domain, the SSO domain can be deleted
- Added support for the HTTP method “report”
- When an SSO image set is updated, changes are updated automatically
- Error codes for RESTful API have been updated – missing REST objects return a 404 error and others return 200 plus an error code
- RESTful API GET responses are consistent with the corresponding SET commands
- Websocket connections are supported
- A new option has been added to the **Always Check Persist** field which allows the saving of persistence changes mid-connection
- Templates allow the re-use of Services which have Content Rules
- Users can specify an alternate port for LDAP servers

34.3 Issues Resolved

PD-1746	Fixed an issue where the Statistics could report a negative value for compression
PD-1704	Fixed an issue where the Web User Interface (WUI) would allow more than 510 extra ports in a Virtual Service

PD-1678	Some security vulnerabilities have been addressed
PD-1676	Fixed an issue with disabling a Real Server with a domain name
PD-1430	Users can use sorry servers with a Virtual Service that has SSL re-encryption enabled

34.4 Known Issues

- A critical vulnerability in the LoadMaster Operating System (LMOS) related to Session Management could allow an unauthorized, remote attacker to bypass security protections, gain system privileges, and execute elevated commands such as **ls**, **ps**, **cat**, and so on, thereby compromising the system. Through this remote execution, in certain cases, exposure of sensitive system data such as certificates, private keys, and other information may be possible.

  Further information can be found here: Mitigation For Remote Access Execution Vulnerability.

- Changing an IPv4 address causes problems with IPv6
- Issues are experienced when polling the LoadMaster with SNMP when the Default Gateway is on a different interface
- Access to the LoadMaster WUI using iPhones is not supported.
- The **Real Servers are Local** option is not working as expected

35 Release 7.0-14c

35.1 Issues Resolved

PD-1754	The OpenSSL version has been upgraded to version 1.0.1g, which is not vulnerable to the HeartBleed bug
PD-1702	Fixed an issue with multiple Virtual Services using group permissions and the same SSO domain
PD-1705	Issue with High Availability (HA) bonding has been resolved
PD-1706	Enabling ESP on an SMTP service will no longer display a spurious error message
PD-1709	Issues with the LDAPS and LDAP StartTLS authentication protocols and SSO server have been resolved
PD-1714	ESP-enabled SMTP services correctly pass traffic

35.2 Known Issues

- A critical vulnerability in the LoadMaster Operating System (LMOS) related to Session Management could allow an unauthorized, remote attacker to bypass security protections, gain system privileges, and execute elevated commands such as **ls**, **ps**, **cat**, and so on, thereby compromising the system. Through this remote execution, in certain cases, exposure of sensitive system data such as certificates, private keys, and other information may be possible.

  Further information can be found here: Mitigation For Remote Access Execution Vulnerability.

- Hyper-V Virtual LoadMaster (VLM) NIC alternate IP address settings do not set properly until the machine is rebooted
- When switching to HA mode from a single unit, changing the local IP when setting up HA results in loss of connectivity to the WUI
- Users may appear multiple times in the blocked user list
- Access to the LoadMaster WUI using iPhones is not supported.
- Cannot install Exchange Virtual Services from a template if existing Virtual Services have been created from a template

36 Release 7.0-14a

36.1 New Features

- Support for RSA multi-factor authentication

36.2 Known Issues

- A critical vulnerability in the LoadMaster Operating System (LMOS) related to Session Management could allow an unauthorized, remote attacker to bypass security protections, gain system privileges, and execute elevated commands such as **ls**, **ps**, **cat**, and so on, thereby compromising the system. Through this remote execution, in certain cases, exposure of sensitive system data such as certificates, private keys, and other information may be possible.

  Further information can be found here: Mitigation For Remote Access Execution Vulnerability.

- Hyper-V Virtual LoadMaster (VLM) NIC alternate IP address settings do not set properly until the machine is rebooted
- When switching to HA mode from a single unit, changing the local IP when setting up HA results in loss of connectivity to the WUI
- Users may appear multiple times in the blocked user list
- Access to the LoadMaster WUI using iPhones is not supported.
- Cannot install Exchange Virtual Services from a template if existing Virtual Services have been created from a template

37 Release 7.0-14

37.1 New Features

- Online checking for software updates
- Support has been implemented for add-on packages
- VMware Tools support
- Support for Edge Security Pack (ESP) phase 2:
  - Customizable login forms
  - Public/private options for ESP login form
  - Support soft lock out for users
  - Additional workloads are supported with ESP
  - RADIUS is an option for the authentication server
- LoadMaster for Amazon Web Services (AWS)
- Templates for VMware Horizon Workspace are available

37.2 Feature Enhancements

- More information is provided when resetting your password using the local console
- The legacy heartbeat option is hidden in the Web User Interface (WUI)
- Wildcard certificate matches are presented in an SNI configuration

37.3 Issues Resolved

PD-890	Issue with using non-alphanumeric characters in automated backup passwords has been resolved
PD-1200	Issue with setting a large cache percentage on high memory LoadMasters has been resolved
PD-1284	Issue with statistics when disabling a Real Server has been resolved
PD-1498	Issue where using preferred host in HA can cause both units to become standby has been resolved
PD-1404	SubVSs honor the “Use for SNAT” setting

PD-1452	Restoring backups to inappropriate devices is prevented, for example restoring a HA backup on a single system
PD-1539	Resolved several minor HA-related issues
PD-1206	Resolved issue related to SNMP and SubVSs

37.4 Known Issues

- A critical vulnerability in the LoadMaster Operating System (LMOS) related to Session Management could allow an unauthorized, remote attacker to bypass security protections, gain system privileges, and execute elevated commands such as **ls**, **ps**, **cat**, and so on, thereby compromising the system. Through this remote execution, in certain cases, exposure of sensitive system data such as certificates, private keys, and other information may be possible.

  Further information can be found here: Mitigation For Remote Access Execution Vulnerability.

- Hyper-V Virtual LoadMaster (VLM) NIC alternate IP address settings do not set properly until the machine is rebooted
- When switching to HA mode from a single unit, changing the local IP when setting up HA results in loss of connectivity to the WUI
- The unblock locked user function may not work in all browsers (there are problems in Chrome and Internet Explorer)
- Users may appear multiple times in the blocked user list
- Access to the LoadMaster WUI using iPhones is not supported.
- Cannot install Exchange Virtual Services from a template if existing Virtual Services have been created from a template

38 Release 7.0-12a

The LM-2500 and LM-3500 are not supported from LoadMaster version 7.0-12a and above. Support for these models, and FIPS models, is offered at version 7.0-10 and below.

38.1 New Features

- SSL Performance Optimizations
- Support for Oracle Sun x86 servers
- Support for HP ProLiant servers
- Support for VMware vSphere 5.5
- Licensing functionality within LoadMaster has been enhanced including the display of the license related information on the LoadMaster WUI home screen and various enhancements to the Automated Licensing Support Infrastructure.
- Windows 2012 R2 Hyper-V Virtual LoadMaster (VLM)
- Idle and session timeout can be set and it is possible to switch between idle and session timeout

38.2 Feature Enhancements

- Additional commands and functionality have been added to the RESTful API
- Additional licensing information has been added to the backup file

38.3 Issues Resolved

PD-797	Issue with the Packet Routing Filter after upgrading licenses has been resolved
PD-839	Improved Layer 4 handling of configuration changes enhancing the generation of SNMP traps has been added
PD-934	Issue with sharing persistency across SubVSs has been resolved
PD-1023	High-Availability failover issue when adding high number of interfaces has been resolved
PD-1043	Issue with Access Control Lists and IPv6 has been resolved
PD-1070	The HA 'Forced Switchover' functionality has been removed
PD-1089	Issue with the Use Address for Server NAT option in new servers has been

	resolved
PD-1094	Issue with using the RESTful API to create a Virtual Service using Adaptive Scheduling has been resolved
PD-452	Issue with VLAN trunking on Hyper-V VLMs has been resolved
PD-1174	Security vulnerability (CVE-2004-0230) resolved. This vulnerability may still be reported after running a security test but this is because the test checks the kernel version. The fix has been backported into the LoadMaster but the kernel version has not been updated which is why the vulnerability is still reported even though it does not exist.
PD-1144	ESP issue with publishing a calendar in Exchange 2013 has been resolved

38.4 Known Issues

- A critical vulnerability in the LoadMaster Operating System (LMOS) related to Session Management could allow an unauthorized, remote attacker to bypass security protections, gain system privileges, and execute elevated commands such as **ls**, **ps**, **cat**, and so on, thereby compromising the system. Through this remote execution, in certain cases, exposure of sensitive system data such as certificates, private keys, and other information may be possible.

  Further information can be found here: Mitigation For Remote Access Execution Vulnerability.

- Access to the LoadMaster WUI using iPhones is not supported.
- The Netconsole IP is not applied immediately to both units of a HA pair
- Automated FTP backups must not contain special characters.
- Cannot immediately set the shared and partner IP addresses for HA if the IP address has been only obtained from DHCP. A workaround for this is to set the IP address again.
- A reboot is required if you add IPv6 as an alternative address, create an IPv6 Virtual Service and then create an Access Control List. The reboot is required before entries can be added to the Access Control List.
- On a GEO LM, it is not possible to specify an alternate address on an interface to receive DNS requests.
- Within a Virtual LoadMaster, the alternative NIC IP address settings are not being picked up until the machine is rebooted.

39 Release 7.0-10i

39.1 Issues Resolved

PD-3643	Cipher list restricted to RC4-SHA to mitigate against POODLE vulnerabilities.

39.2 Known Issues

- A critical vulnerability in the LoadMaster Operating System (LMOS) related to Session Management could allow an unauthorized, remote attacker to bypass security protections, gain system privileges, and execute elevated commands such as **ls**, **ps**, **cat**, and so on, thereby compromising the system. Through this remote execution, in certain cases, exposure of sensitive system data such as certificates, private keys, and other information may be possible.

  Further information can be found here: Mitigation For Remote Access Execution Vulnerability.

- Trunked VLANs are not permitted on Hyper-V VLMs.
- Automated FTP backups must not contain special characters.
- Intermittent issue with encryption ASIC driver under atypical conditions.
- The HA 'Force Switchover' button behaves erratically.

40 Release 7.0-10h

40.1 Issues Resolved

PD-3146	Steps taken to mitigate the following security risk – CVE-2014-3566 (“POODLE”).
PD-3201	Added the option to disable weak SSL ciphers.

40.2 Known Issues

- A critical vulnerability in the LoadMaster Operating System (LMOS) related to Session Management could allow an unauthorized, remote attacker to bypass security protections, gain system privileges, and execute elevated commands such as **ls**, **ps**, **cat**, and so on, thereby compromising the system. Through this remote execution, in certain cases, exposure of sensitive system data such as certificates, private keys, and other information may be possible.

  Further information can be found here: Mitigation For Remote Access Execution Vulnerability.

- Trunked VLANs are not permitted on Hyper-V VLMs.
- Automated FTP backups must not contain special characters.
- Access to the LoadMaster WUI using iPhones is not supported.
- Intermittent issue with encryption ASIC driver under atypical conditions.
- The HA ‘Force Switchover’ button behaves erratically

41 Release 7.0-10g

41.1 Issues Resolved

PD-2976	Steps taken to mitigate the following security risks – CVE-2014-6271 and CVE-2014-7169.

41.2 Known Issues

- A critical vulnerability in the LoadMaster Operating System (LMOS) related to Session Management could allow an unauthorized, remote attacker to bypass security protections, gain system privileges, and execute elevated commands such as **ls**, **ps**, **cat**, and so on, thereby compromising the system. Through this remote execution, in certain cases, exposure of sensitive system data such as certificates, private keys, and other information may be possible.

  Further information can be found here: Mitigation For Remote Access Execution Vulnerability.

- Trunked VLANs are not permitted on Hyper-V VLMs.
- Automated FTP backups must not contain special characters.
- Access to the LoadMaster WUI using iPhones is not supported.
- Intermittent issue with encryption ASIC driver under atypical conditions.
- The HA 'Force Switchover' button behaves erratically

42 Release 7.0-10f

42.1 Issues Resolved

PD-2274	Fixed an issue with the LoadMaster logging process which, in some circumstances, may lead to excessive wear of our Solid State Drives (SSDs)
PD-2376	Added functions to sanitize input in the Web User Interface (WUI) to improve security – fix for CVE-2014-5287 and CVE-2014-5288

42.2 Known Issues

- A critical vulnerability in the LoadMaster Operating System (LMOS) related to Session Management could allow an unauthorized, remote attacker to bypass security protections, gain system privileges, and execute elevated commands such as **ls**, **ps**, **cat**, and so on, thereby compromising the system. Through this remote execution, in certain cases, exposure of sensitive system data such as certificates, private keys, and other information may be possible.

  Further information can be found here: Mitigation For Remote Access Execution Vulnerability.

- Trunked VLANs are not permitted on Hyper-V VLMs.
- Automated FTP backups must not contain special characters.
- Access to the LoadMaster WUI using iPhones is not supported.
- Intermittent issue with encryption ASIC driver under atypical conditions.
- The HA 'Force Switchover' button behaves erratically

43 Release 7.0-10e

43.1 Issues Resolved

PD-2123	Security fix for CVE-2014-0224

43.2 Known Issues

- A critical vulnerability in the LoadMaster Operating System (LMOS) related to Session Management could allow an unauthorized, remote attacker to bypass security protections, gain system privileges, and execute elevated commands such as **ls**, **ps**, **cat**, and so on, thereby compromising the system. Through this remote execution, in certain cases, exposure of sensitive system data such as certificates, private keys, and other information may be possible.

  Further information can be found here: Mitigation For Remote Access Execution Vulnerability.

- Trunked VLANs are not permitted on Hyper-V VLMs.
- Automated FTP backups must not contain special characters.
- Access to the LoadMaster WUI using iPhones is not supported.
- Intermittent issue with encryption ASIC driver under atypical conditions.
- The HA 'Force Switchover' button behaves erratically

44 Release 7.0-10d

44.1 Issues Resolved

PD-1413	Security fix for CVE-2004-0230
PD-1487	Security fix for XSS attack on ESP
PD-1617	Driver update: ixgbe drivers have been updated to version 3.18.7
PD-1925	Fixed an issue where setting up an HA standby unit could cause service interruption in certain cases
PD-1931	Fixed an issue to prevent spurious log messages appearing
PD-1965	Fixed a potential issue where logging into an ESP Virtual Service would be blocked

44.2 Known Issues

- A critical vulnerability in the LoadMaster Operating System (LMOS) related to Session Management could allow an unauthorized, remote attacker to bypass security protections, gain system privileges, and execute elevated commands such as **ls**, **ps**, **cat**, and so on, thereby compromising the system. Through this remote execution, in certain cases, exposure of sensitive system data such as certificates, private keys, and other information may be possible.

  Further information can be found here: Mitigation For Remote Access Execution Vulnerability.

- Trunked VLANs are not permitted on Hyper-V VLMs.
- Automated FTP backups must not contain special characters.
- Access to the LoadMaster WUI using iPhones is not supported.
- Intermittent issue with encryption ASIC driver under atypical conditions.
- The HA 'Force Switchover' button behaves erratically

45 Release 7.0-10

45.1 New Features

- Lync 2013 Templates
- Windows 2012 Hyper-V Virtual LoadMaster (VLM)
- Windows 8 Hyper-V Virtual LoadMaster (VLM)

45.2 Feature Enhancements

- Additional commands have been added to the RESTful API
- A hyperlink within the WUI opens a WUI connection to the other unit within a HA pair
- Enhancements to the ALSI have been implemented
- Statistics collection is configurable
- 'Sorry Server' is available for UDP services

45.3 Issues Resolved

PD-536	Issue with disabling Real Servers has been resolved
PD-537	Issue with RADIUS authorization when not in session mode has been resolved
PD-544	Minor inconsistencies with the display of real server statistics has been resolved
PD-557	Issue with L7 Drain Time has been resolved
PD-570	Added a limit to the size of the files that can be compressed
PD-643	The HTTP 1.1 PATCH method is supported
PD-645	Issue in handling 'SuperHTTP or Source IP Address' persistence method has been resolved
PD-769	Inconsistency in visibility of Add HTTP Headers field has been resolved
PD-774	Issue with configuring UDP 'Sorry Server' has been resolved
PD-785	Issue with use of special characters in the SSO Greeting Message has been resolved
PD-787	Issue with Perform if Flag functionality has been resolved
PD-790	Issue with supporting TLS 1.0 for LoadMaster initiated connections has been resolved
PD-791	Issue with port numbers in returned SNMP values has been resolved

45.4 Known Issues

- A critical vulnerability in the LoadMaster Operating System (LMOS) related to Session Management could allow an unauthorized, remote attacker to bypass security protections, gain system privileges, and execute elevated commands such as **ls**, **ps**, **cat**, and so on, thereby compromising the system. Through this remote execution, in certain cases, exposure of sensitive system data such as certificates, private keys, and other information may be possible.

  Further information can be found here: Mitigation For Remote Access Execution Vulnerability.

- Trunked VLANs are not permitted on Hyper-V VLMs.
- Automated FTP backups must not contain special characters.
- Access to the LoadMaster WUI using iPhones is not supported.
- Intermittent issue with encryption ASIC driver under atypical conditions.
- The HA 'Force Switchover' button behaves erratically

46 Release 7.0-8e

46.1 Feature Enhancements

- Automated Licensing and Support Infrastructure (ALSI) Enhancements

46.2 Issues Resolved

PD-675	Corrected available TLS cipher suite for LM-5305-FIPS
PD-708	SSL Re-encrypt works properly on LM-5305-FIPS
PD-700	Fixed reboot issue when changing service types
PD-739	Additional special characters are allowed in SSO passwords
PD-758	Fixed issue where the initial SSO login would not properly pass query string to the server
PD-581	The " character is allowed in the SSO greeting message

46.3 Known Issues

- A critical vulnerability in the LoadMaster Operating System (LMOS) related to Session Management could allow an unauthorized, remote attacker to bypass security protections, gain system privileges, and execute elevated commands such as **ls**, **ps**, **cat**, and so on, thereby compromising the system. Through this remote execution, in certain cases, exposure of sensitive system data such as certificates, private keys, and other information may be possible.

  Further information can be found here: Mitigation For Remote Access Execution Vulnerability.

- Access to the LoadMaster WUI using iPhones is not supported.
- Warnings (which can be ignored) appear when deploying .ovf files.
- Intermittent issue with encryption ASIC driver under atypical conditions
- Update issues with Real Server statistics
- Intermittent issue with disabling Real Servers
- The HA 'Force Switchover' button behaves erratically

47 Release 7.0-8a

47.1 Feature Enhancements

- Automated Licensing and Support Infrastructure Enhancements

47.2 Issues Resolved

PD-415	Issue with SSOMGR has been resolved

47.3 Known Issues

- A critical vulnerability in the LoadMaster Operating System (LMOS) related to Session Management could allow an unauthorized, remote attacker to bypass security protections, gain system privileges, and execute elevated commands such as **ls**, **ps**, **cat**, and so on, thereby compromising the system. Through this remote execution, in certain cases, exposure of sensitive system data such as certificates, private keys, and other information may be possible.

  Further information can be found here: Mitigation For Remote Access Execution Vulnerability.

- Access to the LoadMaster WUI using iPhones is not supported.
- Warnings (which can be ignored) appear when deploying .ovf files.
- Intermittent issue with encryption ASIC driver under atypical conditions
- Update issues with Real Server statistics
- Intermittent issue with disabling Real Servers
- Cannot enter the " character in the SSO Greeting Message
- The HA 'Force Switchover' button behaves erratically

48 Release 7.0-8

48.1 New Features

- Automated Licensing and Support Infrastructure
- Cisco UCS C Series Support
- Geo Server Load Balancer Feature Pack
- New Virtual LoadMaster Products

48.2 Feature Enhancements

- Configurable login format for ESP

48.3 Issues Resolved

PD-154	Additional characters supported in SNMP community strings
PD-188	Quicksetup help auto-popup issue resolved in the CLI.
PD-327	Compression issue with short content lengths resolved.
PD-335	Issue with simultaneous use of SNMP and 'Drop on Fail' has been corrected
PD-336	Issue with LoadMaster Config viewer is resolved
PD-341	Issue with accessing the WUI while using software FIPS is resolved
PD-386	Can connect to Virtual Services, with persistence enabled, during connection drain time.
PD-389	Minor issues with the Exchange Wizard have been resolved
PD-393	HA issue when creating VLANs under load is resolved.
PD-401	Issue with ESP logs is resolved
PD-414	Issue with weighting of SubVS has been resolved
PD-437	Issue with forwarding emails containing the licensing blob is resolved
PD-446	Issue with LoadMaster 2200 under high load resolved.
PD-449	Resolved Certificate Manager issue in configurations with large number of Virtual Services.
PD-550	mail_util.php is included in srcfiles.

48.4 Known Issues

- A critical vulnerability in the LoadMaster Operating System (LMOS) related to Session Management could allow an unauthorized, remote attacker to bypass security protections, gain system privileges, and execute elevated commands such as **ls**, **ps**, **cat**, and so on, thereby compromising the system. Through this remote execution, in certain cases, exposure of sensitive system data such as certificates, private keys, and other information may be possible.

  Further information can be found here: Mitigation For Remote Access Execution Vulnerability.

- Access to the LoadMaster WUI using iPhones is not supported.
- Warnings (which can be ignored) appear when deploying .ovf files.
- Intermittent issue with encryption ASIC driver under atypical conditions
- Update issues with Real Server statistics
- Intermittent issue with disabling Real Servers
- Cannot enter the " character in the SSO Greeting Message
- The HA 'Force Switchover' button behaves erratically
- Rare segfault with SSOMGR under atypical conditions

49 Release 7.0-6

49.1 New Features

- Quickstart Wizard – Exchange 2010
- RESTful API v.2.0
- Cisco UCS B Series Support
- Call Home - Phase 1

49.2 Feature Enhancements

- After installing or replacing a certificate, there is an option to return to the Virtual Service page
- Quality of Service functionality is configurable within Virtual Services
- The image sets for the ESP login screens support a number of different languages
- The character limit within the Message of the Day has been increased
- When applying a temporary license, feedback is provided if a temporary license has already been applied
- The traceroute and netstat utilities are available debug options
- Bulk disabling of Real Servers is possible
- L7 Transparency is available for selection within a SubVS when the parent Virtual Service uses SSL Acceleration with re-encryption enabled.

49.3 Issues Resolved

PD-371, PD370	Issues configuring eth0 on a 64 bit LoadMaster have been resolved
PD-293	Removed restriction on creating a VLAN with an identifier of 1
PD-270	Issue with deleting VSs in a state of Security Down is resolved
PD-263	Issue with HA time out values resolved
PD-257	Issue with Health Checks on ESP enabled Virtual Services have been resolved
PD-247	To conserve CPU, gathering statistics is restricted to the items displayed on the Home page, unless specified in the Collect All WUI option

PD-246	Issue with Port Following is resolved
PD-231	ACLs working as expected when Virtual Services are set to additional ports
PD-230	Initial maximum cache size on LoadMaster for UCS is within the valid range
PD-188	Within the LoadMaster console, an inappropriate call of Quick Help has been resolved
PD-157	Can configure shared interfaces in the HA setup process before rebooting
PD-140	A failed adaptive health check disables the Real Server
PD-205	SNORT 2.9 rules imports correctly

49.4 Known Issues

- A critical vulnerability in the LoadMaster Operating System (LMOS) related to Session Management could allow an unauthorized, remote attacker to bypass security protections, gain system privileges, and execute elevated commands such as **ls**, **ps**, **cat**, and so on, thereby compromising the system. Through this remote execution, in certain cases, exposure of sensitive system data such as certificates, private keys, and other information may be possible.

  Further information can be found here: Mitigation For Remote Access Execution Vulnerability.

- A page is not delivered when using compression and http content-length is 0 bytes
- Issues may occur with SNMP traffic when the Drop at Drain Time End option is enabled

50 Release 7.0-4

50.1 New Features

- Edge Security Pack: A range of new security features has been added to the LoadMaster.
- The LoadMaster supports the creation and management of SubVSs.
- There is a new dashboard home screen with the capability to display graphical performance information.
- A new license format has been introduced
- A new VLM package, to support VLM installation within an Oracle VirtualBox environment is available

50.2 Feature Enhancements

- MIB files have been updated
- SID and revision information included in IPS logging
- VLAN Separation per Interface
- Support for larger TCP window sizes
- 'Kill switch' is supported on all LoadMaster versions
- LM-R320 has its serial number visible on the WUI
- The Netconsole Host interface is configurable using the WUI

50.3 Issues Resolved

1850	Issue with SMTP STARTTLS when a client sends an EHLO is resolved
2325	Issue with ACL whitelist allowing other IPs is resolved
2584	Issue with switching VS types under load is resolved
2669, 2556	Some reboot issues have been resolved
2657	An issue with caching on Firefox has been resolved
2788	The "-" character is allowed in the DNS Search Domain field
2598	Issues with the MIBS have been resolved

2675	A circular routing problem has been resolved
2278	SNMP trap Source IP has been changed to pre 5.1-48 behaviour
2328	SSL renegotiation can be toggled on/off
2528	SSLv2 is no longer used for LoadMaster initiated SSL connections
2578	An issue with Not Available Redirection XSS has been resolved
2599	The Default IP is displayed on the WUI when DHCP fails
2390	An issue with VS Specific insert X-Clientside header being overwritten by system default has been resolved
2475	The "-" character is allowed in the User Login field
2529	An issue with the Fail on Match functionality has been resolved
2671	An issue with Maximum Cache Size has been resolved

50.4 Known Issues

- A critical vulnerability in the LoadMaster Operating System (LMOS) related to Session Management could allow an unauthorized, remote attacker to bypass security protections, gain system privileges, and execute elevated commands such as **ls**, **ps**, **cat**, and so on, thereby compromising the system. Through this remote execution, in certain cases, exposure of sensitive system data such as certificates, private keys, and other information may be possible.

  Further information can be found here: Mitigation For Remote Access Execution Vulnerability.

- Quick setup Help appears automatically if no IP address is configured on the LM if a VLAN is configured on eth0 and no IP address is assigned to the underlying interface (eth0)

Last Updated Date

This document was last updated on 23 March 2018.

