



# Legacy LoadMaster

## Release Notes

UPDATED: 08 December 2020



## **Copyright Notices**

Copyright © 2002-2020 Kemp Technologies, Inc. All rights reserved. Kemp Technologies and the Kemp Technologies logo are registered trademarks of Kemp Technologies, Inc.

Kemp Technologies, Inc. reserves all ownership rights for the LoadMaster and Kemp 360 product line including software and documentation.

Used, under license, U.S. Patent Nos. 6,473,802, 6,374,300, 8,392,563, 8,103,770, 7,831,712, 7,606,912, 7,346,695, 7,287,084 and 6,970,933

# Table of Contents

---

<b>1 Software Release Notes Introduction .....</b>	<b>11</b>
1.1 Pre-requisites .....	11
1.2 Support .....	11
<b>2 Compatible Products .....</b>	<b>12</b>
<b>3 Release 7.1.35.5 .....</b>	<b>13</b>
3.1 7.1.35.5 - New Features .....	13
3.2 7.1.35.5 - Feature Enhancements .....	13
3.3 7.1.35.5 - Issues Resolved .....	13
3.4 7.1.35.5 - Known Issues .....	13
<b>4 Release 7.1.35.4 .....</b>	<b>17</b>
4.1 7.1.35.4 - Feature Enhancements .....	17
4.2 7.1.35.4 - Issues Resolved .....	17
4.3 7.1.35.4 - Known Issues .....	18
<b>5 Release 7.1.35.3 .....</b>	<b>21</b>
5.1 Feature Enhancements .....	21
5.2 Issues Resolved .....	21
5.3 Known Issues .....	22
<b>6 Release 7.1.35.2 .....</b>	<b>24</b>
6.1 Issues Resolved .....	24
6.2 7.1.35.2 - Known Issues .....	24
<b>7 Release 7.1.35 .....</b>	<b>25</b>

---

7.1 New Features .....	25
7.2 Feature Enhancements .....	26
7.3 Issues Resolved .....	26
7.4 Known Issues .....	29
<b>8 Release 7.1.34.1 .....</b>	<b>33</b>
8.1 New Features .....	33
8.2 Feature Enhancements .....	33
8.3 Issues Resolved .....	35
8.4 Known Issues .....	38
<b>9 Release 7.1-32a .....</b>	<b>40</b>
9.1 New Features .....	40
9.2 Feature Enhancements .....	40
9.3 Issues Resolved .....	41
9.4 Known Issues .....	43
<b>10 Release 7.1-30a .....</b>	<b>45</b>
10.1 Feature Enhancements .....	45
10.2 Issues Resolved .....	45
10.3 7.1-30a - Known Issues .....	45
<b>11 Release 7.1-30 .....</b>	<b>46</b>
11.1 New Features .....	46
11.2 Feature Enhancements .....	46
11.3 Issues Resolved .....	47

---

11.4 Known Issues .....	48
<b>12 Release 7.1-28b .....</b>	<b>50</b>
12.1 Feature Enhancements .....	50
12.2 Issues Resolved .....	50
12.3 Known Issues .....	50
<b>13 Release 7.1-28a .....</b>	<b>52</b>
13.1 New Features .....	52
13.2 Feature Enhancements .....	52
13.3 Issues Resolved .....	52
13.4 Known Issues .....	52
<b>14 Release 7.1-28 .....</b>	<b>54</b>
14.1 New Features .....	54
14.2 Feature Enhancements .....	54
14.3 Issues Resolved .....	55
14.4 Known Issues .....	57
<b>15 Release 7.1-26c .....</b>	<b>59</b>
15.1 Issues Resolved .....	59
15.2 7.1-26c - Known Issues .....	59
<b>16 Release 7.1-26 .....</b>	<b>60</b>
16.1 New Features .....	60
16.2 Feature Enhancements .....	60
16.3 Issues Resolved .....	61

---

16.4 Known Issues .....	62
<b>17 Release 7.1-24b .....</b>	<b>64</b>
17.1 New Features .....	64
17.2 Feature Enhancements .....	64
17.3 Issues Resolved .....	64
17.4 Known Issues .....	64
<b>18 Release 7.1-24a .....</b>	<b>66</b>
18.1 New Features .....	66
18.2 Feature Enhancements .....	66
18.3 Issues Resolved .....	66
18.4 Known Issues .....	68
<b>19 Release 7.1-22b .....</b>	<b>69</b>
19.1 Feature Enhancements .....	69
19.2 Issues Resolved .....	69
19.3 Known Issues .....	69
<b>20 Release 7.1-22 .....</b>	<b>71</b>
20.1 New Features .....	71
20.2 Feature Enhancements .....	71
20.3 Issues Resolved .....	72
20.4 Known Issues .....	72
<b>21 Release 7.1-20d .....</b>	<b>74</b>
21.1 Feature Enhancements .....	74

---

21.2 Known Issues .....	74
<b>22 Release 7.1-20a .....</b>	<b>75</b>
22.1 New Features .....	75
22.2 Feature Enhancements .....	75
22.3 Issues Resolved .....	75
22.4 Known Issues .....	77
<b>23 Release 7.1-18b .....</b>	<b>78</b>
23.1 New Features .....	78
23.2 Feature Enhancements .....	78
23.3 Issues Resolved .....	78
23.4 Known Issues .....	80
<b>24 Release 7.1-16b .....</b>	<b>81</b>
24.1 New Features .....	81
24.2 Issues Resolved .....	81
24.3 Known Issues .....	81
<b>25 Release 7.1-16 .....</b>	<b>82</b>
25.1 New Features .....	82
25.2 Feature Enhancements .....	82
25.3 Issues Resolved .....	82
25.4 Known Issues .....	83
<b>26 Release 7.0-14c .....</b>	<b>84</b>
26.1 Issues Resolved .....	84

---

26.2 Known Issues .....	84
<b>27 Release 7.0-14a .....</b>	<b>86</b>
27.1 New Features .....	86
27.2 Known Issues .....	86
<b>28 Release 7.0-14 .....</b>	<b>87</b>
28.1 New Features .....	87
28.2 Feature Enhancements .....	87
28.3 Issues Resolved .....	87
28.4 Known Issues .....	88
<b>29 Release 7.0-12a .....</b>	<b>89</b>
29.1 New Features .....	89
29.2 Feature Enhancements .....	89
29.3 Issues Resolved .....	89
29.4 Known Issues .....	90
<b>30 Release 7.0-10i .....</b>	<b>92</b>
30.1 Issues Resolved .....	92
30.2 Known Issues .....	92
<b>31 Release 7.0-10h .....</b>	<b>93</b>
31.1 Issues Resolved .....	93
31.2 Known Issues .....	93
<b>32 Release 7.0-10g .....</b>	<b>94</b>
32.1 Issues Resolved .....	94



---

32.2 Known Issues .....	94
<b>33 Release 7.0-10f .....</b>	<b>95</b>
33.1 Issues Resolved .....	95
33.2 Known Issues .....	95
<b>34 Release 7.0-10e .....</b>	<b>96</b>
34.1 Issues Resolved .....	96
34.2 Known Issues .....	96
<b>35 Release 7.0-10d .....</b>	<b>97</b>
35.1 Issues Resolved .....	97
35.2 Known Issues .....	97
<b>36 Release 7.0-10 .....</b>	<b>98</b>
36.1 New Features .....	98
36.2 Feature Enhancements .....	98
36.3 Issues Resolved .....	98
36.4 Known Issues .....	99
<b>37 Release 7.0-8e .....</b>	<b>100</b>
37.1 Feature Enhancements .....	100
37.2 Issues Resolved .....	100
37.3 Known Issues .....	100
<b>38 Release 7.0-8a .....</b>	<b>102</b>
38.1 Feature Enhancements .....	102
38.2 Issues Resolved .....	102

---

38.3 Known Issues .....	102
<b>39 Release 7.0-8 .....</b>	<b>103</b>
39.1 New Features .....	103
39.2 Feature Enhancements .....	103
39.3 Issues Resolved .....	103
39.4 Known Issues .....	104
<b>40 Release 7.0-6 .....</b>	<b>105</b>
40.1 New Features .....	105
40.2 Feature Enhancements .....	105
40.3 Issues Resolved .....	105
40.4 Known Issues .....	106
<b>41 Release 7.0-4 .....</b>	<b>107</b>
41.1 New Features .....	107
41.2 Feature Enhancements .....	107
41.3 Issues Resolved .....	107
41.4 Known Issues .....	108
<b>Last Updated Date .....</b>	<b>109</b>

# 1 Software Release Notes Introduction

This document provides release notes for legacy LoadMaster firmware versions.

To see release notes for newer firmware versions, go to the **LoadMaster Release Notes** section of the [Kemp Documentation Page](#).

---

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 <https://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 <https://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: <https://kemptechnologies.com/support>

## 2 Compatible Products

- LM-X15
- LM-X3
- LM-2400
- LM-2600
- LM-3400
- LM-3600
- LM-5300
- LM-5400
- LM-5000
- LM-5600
- LM-8000
- LM-8020 (supported on version 7.1-30 and above)
- LM-R320
- VLM-200
- LM-3000
- LM-4000
- VLM-1000
- VLM-2000
- VLM-3000
- VLM-5000
- 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
- LoadMaster for AWS
- LoadMaster for Azure

# 3 Release 7.1.35.5

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

## 3.1 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.

## 3.2 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).

## 3.3 7.1.35.5 - Issues Resolved

---

PD-11023	<p>Previously, a critical vulnerability (CVE-2018-9091) 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 <b>ls</b>, <b>ps</b>, <b>cat</b>, 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.</p> <p>Now, this vulnerability has been mitigated against with more stringent security checks. Further information can be found here: <a href="#">Mitigation For Remote Access Execution Vulnerability</a>.</p>
----------	--

---

## 3.4 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 <b>Inspect HTML POST Request Content</b> 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 <b>Process Responses</b> 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 <b>HTTP/1.1 500 Internal Server Error</b> 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 <b>showiface</b> 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 <b>removecountry</b> API response error message.
PD-9553	There is no API command to disable secure NTP mode.
PD-9539	Issues with the PowerShell <b>New-GeoCluster</b> command in a specific scenario.
PD-9525	The RESTful API returns the value of the <b>failtime</b> 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 <b>VSIndex</b> parameter is missing in some API calls.
PD-9575	There are issues with some <b>accontrol</b> API commands.
PD-10160	The API commands to reset the CPU and network graphs do not work.



# 4 Release 7.1.35.4

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

## 4.1 7.1.35.4 - Feature Enhancements

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

## 4.2 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 <b>Drop Connections on RS failure</b> 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 <b>aclcontrol</b> API commands.
PD-9790	The <b>CheckPort</b> and <b>CheckPattern</b> API parameters can be unset using the API.
PD-9773	Fixed an issue that showed different statuses for disabled Virtual Services in the API.

### 4.3 7.1.35.4 - Known Issues

PD-11023	<p>A critical vulnerability (CVE-2018-9091) 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 <b>ls</b>, <b>ps</b>, <b>cat</b>, 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.</p> <p>Further information can be found here: <a href="#">Mitigation For Remote Access Execution Vulnerability</a>.</p>
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 <b>showiface</b> 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 <b>removecountry</b> API response error message.
PD-9553	There is no API command to disable secure NTP mode.
PD-9539	Issues with the PowerShell <b>New-GeoCluster</b> command in a specific scenario.
PD-9525	The RESTful API returns the value of the <b>failtime</b> 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 <b>VSIndex</b> parameter is missing in some API calls.
PD-9575	There are issues with some <b>aclcontrol</b> API commands.
PD-10160	The API commands to reset the CPU and network graphs do not work.

# 5 Release 7.1.35.3

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

## 5.1 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.

## 5.2 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.

## 5.3 Known Issues

PD-11023	<p>A critical vulnerability (CVE-2018-9091) 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 <b>ls</b>, <b>ps</b>, <b>cat</b>, 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.</p> <p>Further information can be found here: <a href="#">Mitigation For Remote Access Execution Vulnerability</a>.</p>
PD-8725	<b>Proximity</b> and <b>Location Based</b> scheduling do not work with IPv6 source addresses.
PD-9950	LoadMaster VNF HA does not work on LoadMaster versions 7.1.35. <i>n</i> and 7.2.36. <i>n</i> . 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.

# 6 Release 7.1.35.2

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

## 6.1 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.

## 6.2 7.1.35.2 - Known Issues

PD-11023	<p>A critical vulnerability (CVE-2018-9091) 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 <b>ls</b>, <b>ps</b>, <b>cat</b>, 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.</p> <p>Further information can be found here: <a href="#">Mitigation For Remote Access Execution Vulnerability</a>.</p>
PD-8725	<p><b>Proximity</b> and <b>Location Based</b> scheduling do not work with IPv6 source addresses.</p>



# 7 Release 7.1.35

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

---

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

---

## 7.1 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).

## 7.2 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.

## 7.3 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 dhcpd 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	OCSF 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 shows 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.

## 7.4 Known Issues

PD-11023	<p>A critical vulnerability (CVE-2018-9091) 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 <b>ls</b>, <b>ps</b>, <b>cat</b>, 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.</p> <p>Further information can be found here: <a href="#">Mitigation For Remote Access Execution Vulnerability</a>.</p>
PD-8725	<b>Proximity</b> and <b>Location Based</b> scheduling do not work with

IPv6 source addresses.	
PD-9950	LoadMaster VNF HA does not work on LoadMaster versions 7.1.35. <i>n</i> and 7.2.36. <i>n</i> . 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-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.



# 8 Release 7.1.34.1

Refer to the sections below for details about firmware version 7.1.34.1. This was released on 18<sup>th</sup> 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.

---

## 8.1 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

## 8.2 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:
  - Dell Wyse vWorkspace
  - 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.

## 8.3 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.

## 8.4 Known Issues

PD-11023	A critical vulnerability (CVE-2018-9091) 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 <b>ls</b> , <b>ps</b> , <b>cat</b> , 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: <a href="#">Mitigation For Remote Access Execution Vulnerability</a> .
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.

---

# 9 Release 7.1-32a

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

## 9.1 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.

## 9.2 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:
  - AD FS v3
  - DirectAccess



- Fujifilm Synapse
  - Skype for Business
  - Greenway PrimeSuite
  - Epicor ERP
  - 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.

## 9.3 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.

## 9.4 Known Issues

PD-11023	<p>A critical vulnerability (CVE-2018-9091) 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 <b>ls</b>, <b>ps</b>, <b>cat</b>, 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.</p>
----------	--

---

	Further information can be found here: <a href="#">Mitigation For Remote Access Execution Vulnerability</a> .
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.

---

# 10 Release 7.1-30a

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

## 10.1 Feature Enhancements

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

## 10.2 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.

## 10.3 7.1-30a - Known Issues

PD-11023	<p>A critical vulnerability (CVE-2018-9091) 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 <b>ls</b>, <b>ps</b>, <b>cat</b>, and so on, thereby compromising the system.</p> <p>Through this remote execution, in certain cases, exposure of sensitive system data such as certificates, private keys, and other information may be possible.</p> <p>Further information can be found here: <a href="#">Mitigation For Remote Access Execution Vulnerability</a>.</p>
----------	---

# 11 Release 7.1-30

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

## 11.1 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

## 11.2 Feature Enhancements

- Content switching based on request payload is supported.
- The total number of allowed concurrent administrative login 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.

### 11.3 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.

## 11.4 Known Issues

PD-11023	A critical vulnerability (CVE-2018-9091) 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 <b>ls</b> , <b>ps</b> , <b>cat</b> , 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: <a href="#">Mitigation For Remote Access Execution Vulnerability</a> .	
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.

# 12 Release 7.1-28b

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

## 12.1 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.

## 12.2 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.

## 12.3 Known Issues

PD-11023	<p>A critical vulnerability (CVE-2018-9091) 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 <b>ls</b>, <b>ps</b>, <b>cat</b>, 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.</p> <p>Further information can be found here: <a href="#">Mitigation For Remote Access Execution Vulnerability</a>.</p>
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.

# 13 Release 7.1-28a

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

## 13.1 New Features

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

## 13.2 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.

## 13.3 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) <b>Delegate to Server</b> 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.

## 13.4 Known Issues

PD-11023	A critical vulnerability (CVE-2018-9091) 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 <b>ls</b> , <b>ps</b> , <b>cat</b> , 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: <a href="#">Mitigation For Remote Access Execution Vulnerability</a> .
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

# 14 Release 7.1-28

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

## 14.1 New Features

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

## 14.2 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

## 14.3 Issues Resolved

Vulnerability - XSS	
PD-4195	Credited to – Francesco Perna (CVE submitted)
Vulnerability - XSRF	
PD-4196	Credited to – Francesco Perna (CVE submitted)
Vulnerability - OS Command Injection	
PD-4198	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.

## 14.4 Known Issues

PD-11023	<p>A critical vulnerability (CVE-2018-9091) 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 <b>ls</b>, <b>ps</b>, <b>cat</b>, 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.</p> <p>Further information can be found here: <a href="#">Mitigation For Remote Access Execution Vulnerability</a>.</p>
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 <b>Miscellaneous Params</b> 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.

# 15 Release 7.1-26c

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

## 15.1 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

---

## 15.2 7.1-26c - Known Issues

---

PD-11023	<p>A critical vulnerability (CVE-2018-9091) 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 <b>ls</b>, <b>ps</b>, <b>cat</b>, and so on, thereby compromising the system.</p> <p>Through this remote execution, in certain cases, exposure of sensitive system data such as certificates, private keys, and other information may be possible.</p> <p>Further information can be found here: <a href="#">Mitigation For Remote Access Execution Vulnerability</a>.</p>
----------	---

---

# 16 Release 7.1-26

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

## 16.1 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

## 16.2 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 from 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

## 16.3 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)
	Vulnerability - Cross Site Request Forgery
PD-3781	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.

## 16.4 Known Issues

PD-11023	<p>A critical vulnerability (CVE-2018-9091) 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 <b>ls</b>, <b>ps</b>, <b>cat</b>, 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.</p> <p>Further information can be found here: <a href="#">Mitigation For Remote Access Execution Vulnerability</a>.</p>
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.

# 17 Release 7.1-24b

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

## 17.1 New Features

- Free LoadMaster product

## 17.2 Feature Enhancements

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

## 17.3 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 <b>Audit Only</b> mode.
PD-3330	Fixed an issue which caused the URL to be improperly encoded when using <b>Form Based</b> authentication.
PD-3843	Fixed an issue where Web Application Firewall (WAF) rule updates caused the LoadMaster backup file size to increase.

## 17.4 Known Issues

PD-11023	A critical vulnerability (CVE-2018-9091) 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 <b>ls</b> , <b>ps</b> , <b>cat</b> , 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: <a href="#">Mitigation For Remote Access</a>
----------	--



<u>Execution Vulnerability.</u>	
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 <b>cat</b> command) and upload the combined file.

# 18 Release 7.1-24a

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

## 18.1 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

## 18.2 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.

## 18.3 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 <b>TLStyle</b> RESTful API parameter not being saved.
PD-3160	Fixed an issue with the <b>modmap</b> 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 <b>addmap</b> RESTful API command works in all scenarios.

---

PD-3075	A superfluous error message, which displayed when setting the <b>isolateips</b> parameter using the <b>ModifyFQDN</b> command, has been removed.
---------	--

---

## 18.4 Known Issues

---

PD-11023	<p>A critical vulnerability (CVE-2018-9091) 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 <b>ls</b>, <b>ps</b>, <b>cat</b>, 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.</p> <p>Further information can be found here: <a href="#">Mitigation For Remote Access Execution Vulnerability</a>.</p>
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.

---

# 19 Release 7.1-22b

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

## 19.1 Feature Enhancements

- Improved logs for SSL thread limit.

## 19.2 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.

## 19.3 Known Issues

PD-11023	<p>A critical vulnerability (CVE-2018-9091) 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 <b>ls</b>, <b>ps</b>, <b>cat</b>, 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.</p> <p>Further information can be found here: <a href="#">Mitigation For Remote Access Execution Vulnerability</a>.</p>
PD-2182	<p>When <b>Permitted Groups</b> are set for ESP, users receive an incorrect credential prompt at the forms-based login when the LoadMaster contacts child domains for user authentication.</p>

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 <b>modmap</b> 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 <b>addmap</b> RESTful API command does not work when the <b>Selection Criteria</b> is set to <b>Real Server Load</b> .
PD-3075	A superfluous error message appears when you attempt to set the <b>isolateips</b> parameter using the PowerShell <b>ModifyFQDN</b> command.
PD-2992	The temperature on the <b>Statistics</b> 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.

# 20 Release 7.1-22

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

## 20.1 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

## 20.2 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.

## 20.3 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 <b>aclcontrol</b> 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 <b>Use for GEO</b> option is enabled on the interface.
PD-3199	Steps taken to mitigate the following security risk – CVE-2014-3566 (“POODLE”)

## 20.4 Known Issues

PD-11023	A critical vulnerability (CVE-2018-9091) 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 <b>ls</b> , <b>ps</b> , <b>cat</b> , and so on, thereby compromising the system. Through this remote execution, in
----------	--



	<p>certain cases, exposure of sensitive system data such as certificates, private keys, and other information may be possible.</p> <p>Further information can be found here: <a href="#">Mitigation For Remote Access Execution Vulnerability</a>.</p>
PD-2182	When <b>Permitted Groups</b> 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 <b>modmap</b> 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 <b>addmap</b> RESTful API command does not work when the <b>Selection Criteria</b> is set to <b>Real Server Load</b> .
PD-3075	A superfluous error message appears when you attempt to set the <b>isolateips</b> parameter using the PowerShell <b>ModifyFQDN</b> command.
PD-2992	The temperature on the <b>Statistics</b> 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.

# 21 Release 7.1-20d

## 21.1 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.

## 21.2 Known Issues

PD-11023	<p>A critical vulnerability (CVE-2018-9091) 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 <b>ls</b>, <b>ps</b>, <b>cat</b>, 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.</p> <p>Further information can be found here: <a href="#">Mitigation For Remote Access Execution Vulnerability</a>.</p>
PD-2182	When <b>Permitted Groups</b> 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 <b>accontrol</b> 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.

# 22 Release 7.1-20a

## 22.1 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.

## 22.2 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

## 22.3 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 <b>Allow Administrative WUI Access</b> 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

## 22.4 Known Issues

- A critical vulnerability (CVE-2018-9091) 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.

# 23 Release 7.1-18b

## 23.1 New Features

- VMware vCenter Operations Management Pack released
- Azure High Availability (HA) enhancements
  - Azure HA mode health check
  - Azure HA mode remote synchronization
  - 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

## 23.2 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

## 23.3 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

## 23.4 Known Issues

- A critical vulnerability (CVE-2018-9091) 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



# 24 Release 7.1-16b

## 24.1 New Features

- Support added for Amazon Web Services (AWS)

## 24.2 Issues Resolved

---

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

---

## 24.3 Known Issues

- A critical vulnerability (CVE-2018-9091) 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

# 25 Release 7.1-16

## 25.1 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

## 25.2 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

## 25.3 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

## 25.4 Known Issues

- A critical vulnerability (CVE-2018-9091) 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

# 26 Release 7.0-14c

## 26.1 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

## 26.2 Known Issues

- A critical vulnerability (CVE-2018-9091) 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

# 27 Release 7.0-14a

## 27.1 New Features

- Support for RSA multi-factor authentication

## 27.2 Known Issues

- A critical vulnerability (CVE-2018-9091) 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

# 28 Release 7.0-14

## 28.1 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

## 28.2 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

## 28.3 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

## 28.4 Known Issues

- A critical vulnerability (CVE-2018-9091) 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



# 29 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.

---

## 29.1 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

## 29.2 Feature Enhancements

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

## 29.3 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

## 29.4 Known Issues

- A critical vulnerability (CVE-2018-9091) 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.

# 30 Release 7.0-10i

## 30.1 Issues Resolved

---

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

---

## 30.2 Known Issues

- A critical vulnerability (CVE-2018-9091) 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.

# 31 Release 7.0-10h

## 31.1 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.

---

## 31.2 Known Issues

- A critical vulnerability (CVE-2018-9091) 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

# 32 Release 7.0-10g

## 32.1 Issues Resolved

---

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

---

## 32.2 Known Issues

- A critical vulnerability (CVE-2018-9091) 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

# 33 Release 7.0-10f

## 33.1 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

## 33.2 Known Issues

- A critical vulnerability (CVE-2018-9091) 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

# 34 Release 7.0-10e

## 34.1 Issues Resolved

---

PD-2123 Security fix for CVE-2014-0224

---

## 34.2 Known Issues

- A critical vulnerability (CVE-2018-9091) 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



# 35 Release 7.0-10d

## 35.1 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

## 35.2 Known Issues

- A critical vulnerability (CVE-2018-9091) 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

# 36 Release 7.0-10

## 36.1 New Features

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

## 36.2 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

## 36.3 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

## 36.4 Known Issues

- A critical vulnerability (CVE-2018-9091) 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

# 37 Release 7.0-8e

## 37.1 Feature Enhancements

- Automated Licensing and Support Infrastructure (ALSI) Enhancements

## 37.2 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

## 37.3 Known Issues

- A critical vulnerability (CVE-2018-9091) 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

# 38 Release 7.0-8a

## 38.1 Feature Enhancements

- Automated Licensing and Support Infrastructure Enhancements

## 38.2 Issues Resolved

---

PD-415 Issue with SSOMGR has been resolved

---

## 38.3 Known Issues

- A critical vulnerability (CVE-2018-9091) 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

# 39 Release 7.0-8

## 39.1 New Features

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

## 39.2 Feature Enhancements

- Configurable login format for ESP

## 39.3 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.

---

## 39.4 Known Issues

- A critical vulnerability (CVE-2018-9091) 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



# 40 Release 7.0-6

## 40.1 New Features

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

## 40.2 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.

## 40.3 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

## 40.4 Known Issues

- A critical vulnerability (CVE-2018-9091) 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

# 41 Release 7.0-4

## 41.1 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

## 41.2 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

## 41.3 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

## 41.4 Known Issues

- A critical vulnerability (CVE-2018-9091) 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 08 December 2020.