KEMP 360 Central Release Notes

Release Notes

KEMP 360 Central Release Notes

Table of Contents

1 Installing and Upgrading KEMP 360 Central

First-time installation of KEMP 360 Central is supported on a number of platforms. In addition to reading these Release Notes, please also read and follow the Installation Guide for your platform, available from the KEMP Documentation Library. Expand the **KEMP 360** link at the top left of the library contents and then click on the installation guide for your platform.

This document applies to KEMP 360 Central. For documentation on configuring LoadMaster, LMOS release notes, information on LMOS backup archive content, or other LoadMaster-specific issues, please refer to the LoadMaster documentation from the KEMP Documentation Library.

1.1 Supported Upgrade Paths

Upgrading directly to the latest version of KEMP 360 Central is supported from **Version 1.9.0.1403** and later releases. For details on the upgrade path to the current release from all past releases, please see the section **Upgrade Path to the Latest Release**.

1.2 Before You Begin

The following notes and subsections list requirements and recommendations for installing and using KEMP 360 Central:

- Any device that you want to add to KEMP 360 Central must be located on a network that can be reached from the KEMP 360 Central instance.
- The person performing a fresh install or upgrade of KEMP 360 Central should be familiar with network administration best practices within their organization and possess an intermediate level of general network and system administration knowledge.
- For the best user experience, KEMP recommends using Google Chrome to access the KEMP 360 Central UI. Other browsers -- Firefox, Safari, Edge, and Internet Explorer -- are also supported.

1.2.1 LMOS Version Support

We strongly recommend that for optimal performance and usability, all LoadMasters managed by KEMP 360 Central are running LMOS **Version 7.1.35**, or a later release.

Older LMOS releases can be managed from KEMP 360 Central, but will experience the following operational limitations:

- LMOS releases prior to **7.1.35** do not support certificate authentication when logging in via the API; KEMP 360 Central will fall back to basic authentication for these LoadMasters.
- LMOS releases prior to **7.1.34** also do not report network interface information and statistics. Because of these and other limitations in these releases of LMOS, we recommend that you do not add more than 50 LoadMasters running releases prior to **7.1.34**.
- LMOS releases prior to **7.1.30b** also report fewer overall statistics.

1.2.2 Virtual Machine Requirements

As of version 1.25.2, the default minimum Virtual Machine (VM) provisioning requirements for new installs were updated as follows:

Resource	V1.23 and earlier firmware	V1.25.2 and later firmware
CPU	2 cores	4 cores
RAM	4 GB	8 GB
Disk storage	40 GB	250 GB

Upgrading to version 1.25.2 and later releases does not update existing VM resources. To modify your current VM configuration to conform to the above minimum values, contact KEMP Support.

1.2.3 System Capacity

A single instance of KEMP 360 Central can host a maximum of 600 managed devices, with a combined total of 18000 resources defined on those devices (Virtual Services, SubVSs, and Real Servers). KEMP 360 central polls these devices regularly for availability and configuration status:

- **Availability status** of managed devices and the load balancing objects defined on them (Virtual Services, SubVSs, and Real Servers) is updated every minute (60 seconds).
- **Configuration status** of managed devices and services is updated every hour (60 minutes). Please note that:
    - If a configuration change is made from KEMP 360 Central, the change is reflected immediately in the KEMP 360 Central UI.
    - For LoadMaster devices, you can also request an immediate configuration update using the **Request Update button** found on the LoadMaster's **System Configuration** tab in the KEMP 360 Central UI.

1.3 Upgrade Instructions

To update KEMP 360 Central to the latest firmware version:

1. Click the **Settings and Configuration** icon (the gear icon) at the bottom-left corner of the UI.

2. Click **Firmware Management**.

3. Click **Select Firmware** and choose the desired update image.

4. Click **Upload**; once the image is uploaded to KEMP 360 Central, the Install button appears.

5. Click **Install** and then click **Yes** in the confirmation popup that appears. The text **Updating...** appears in the accordion button to indicate that the update process has begun. Do not make

any further attempt to use the UI until the system has automatically rebooted, which will take a few minutes. Upon completing the update, the login screen is displayed.

6. Ensure you clear your browser cache before logging into KEMP 360 Central after the upgrade. This is to ensure that the browser downloads the latest UI code from Central.

1.4 Monitoring LoadMaster HA from KEMP 360 Central

Starting with Version 1.19, KEMP 360 Central can be configured to monitor two LoadMasters in HA mode as an HA pair. Please see the **Appendix: Quick Start for Monitoring LoadMaster HA** for more information.

1.5 Getting Help

If you experience issues when installing or upgrading to this release of KEMP 360 Central that can't be resolved by consulting this document or the installation guides available from the Documentation Library, please visit the Support Web Portal to look for help from our user community, access KEMP's Knowledge Base, or submit a support request.

To submit a support request via the Support Portal, please have your KEMP ID and password available. After you file a request, a KEMP Support Engineer will contact you promptly.

2 Version 1.27

Version 1.27 of KEMP 360 Central was released in September 2018 and is a feature and bug-fix release. It contains the new features, resolved issues, and known issues described in the following subsections.

2.1 New Features

Restricting UI Access to Specific IP Addresses

A new 'whitelisting' capability has been added that allows the administrator to specify the source IP addresses and subnets from which UI access will be allowed:

- By default, the system allows access from any IP address that has a route to KEMP 360 Central – as in previous releases.
- Using controls found under **Settings and Configuration > UI Access Control**, you can limit UI access to specific IP addresses, or use CIDR notation to limit access to a range of IP addresses.
- As a lockout protection mechanism, the IP address from which the UI is being accessed to modify the whitelist is always added to the whitelist, even if it is not specified by the user.
- The whitelist applies to UI access only. API access to KEMP 360 Central remains open to any network that has a route to KEMP 360 Central, as in previous releases. This is required to support API access from all managed devices.

LoadMaster Certificate Backup

The Backup and Restore capability now supports creating a backup archive of the SSL certificates installed on a LoadMaster, and restoring those certificates to a LoadMaster:

- When creating a backup archive, the user is now prompted to back up the system configuration only, the SSL certificates only, or both.
- When selecting a backup archive to restore to a LoadMaster, the list now indicates whether an archive contains the system configuration only, certificates only, or both.
- When choosing an archive that has both configuration and certificates, you can choose to restore either configuration or certificates, or both.
- Any backup archive can be downloaded to your local system from KEMP 360 Central in a ZIP file, which will contain a configuration archive, a certificate archive, or both. These can be extracted from the ZIP file and applied to a LoadMaster outside of KEMP 360 Central, using either the LoadMaster WUI or the LMOS API.
  - Note that the ability to upload backup archives from your local system to KEMP 360 Central remains as in previous releases: that is, you can upload a configuration-only archive and it will be recognized by the system. Certificate archives and combined configuration and certificate archives, however, will be accepted by the UI/API and uploaded to the system, but it will produce an error when applied to a LoadMaster.

UI Performance Improvements

The UI has been enhanced to provide better overall performance under a variety of workloads, and to reduce response times for all data queries.

Statistics Gathering Performance Improvements

The process used to poll managed devices for statistics gathering has been enhanced to provide better overall performance and more efficient management of polling activities, especially in larger configurations.

System Capacity Enhancements

With Version 1.27, system capacity has been increased as follows:

- The maximum number of managed devices has been increased to 600 devices.
- The maximum number of managed resources (Virtual Services, SubVSs, Real Servers) has been increased to 18000.

2.2 Issues Resolved

The following are the major issues observed in previous releases that are resolved in this release.

ID	Description
KTS-5168	Fixed an issue that could cause a blank UI page to be displayed after the system is upgraded and rebooted.
KTS-5127	Addressed an issue on installation and licensing where the licensing page gets reset and form data is lost when the **License Now** button is clicked.
KTS-4517	Modified dashboard behavior so that SubVSs are not counted in either the administratively disabled service widget or virtual service status widget – only Virtual Services (VSs) are counted.
KTS-4273	Fixed an issue where a rebooting device is still shown as 'up' in the left frame after a reboot is requested; the icon now changes immediately to show the system is rebooting.
KTS-3695	Enhanced the network tree search facility to search on full or partial network and device nicknames (in addition to the current IP address search).
KTS-3587	Fixed an issue where disabling a Real Server on LoadMaster does not get correctly reflected on KEMP 360 Central.
KTS-3537	Modified dashboard behavior so that real servers under an administratively disabled VS are also shown as disabled.
KTS-2720	Fixed an issue where the **HTTP Method** field displays a blank value for HTTP/S health checks even when there is actual data to display.
KTS-	Fixed issues in the dashboard where a disabled VS is shown as 'down'.

2837

2.3 Known Issues

The following list includes the most serious known issues in the product. If you experience an issue that is not on this list, contact KEMP Support for further information.

ID	Description
KTS-5059 KTS-3876	The outbound proxy functionality (**Settings and Configuration > Proxy Settings**) is broken and does not work. It has been removed and will be provided again in a future release.
KTS-4567	An unmanaged device is not polled immediately upon first contact from KEMP 360 Central. This means that some operations on such a device (for example, **VS Motion Migrate**) cannot be performed until the first time the device is polled for configuration (which occurs every 60 minutes), or until you manually poll the device using the **Update** button on the device's **Monitoring** page.
KTS-4542	When a LoadMaster has been licensed by Central, the user must edit the device definition and add the device's credentials. Once the credentials are added, however, the device configuration is not automatically polled – the user has to wait until the next configuration poll occurs to see any config data for the device. That could be up to one hour later. Instead, the device should be polled immediately for configuration when credentials are added.
KTS-4541	It is possible, after a series of deletions and additions, for statistics for a deleted LoadMaster to be attributed to a LoadMaster created after the deletion occurred. This is due to ID reuse on the LoadMaster. While this has no impact on aggregate statistics reporting, it does mean that statistics attributed to a new device may have timestamps showing a date and/or time before that device was added to KEMP 360 Central.
KTS-4402	On some browsers, the scrollbar on the **System Configuration** screen may not appear at the lowest supported resolution for the Central User Interface (UI) (1366x768). The workaround is to use a higher resolution, or close the collapsible menus so the scrollbar is not needed.
KTS-4341	In the log viewer, AWS-ELB devices are not displayed in the device selection drop-down, so AWS-ELB logs cannot be viewed.
KTS-4299	When viewing third-party F5 device logs in the log viewer, the real servers on the F5 device are not displayed in the search text box.

KTS-3876	When KEMP 360 Central's **Proxy Settings** for outgoing connections (**Settings and Configuration > System Settings > Proxy Settings**) are set or unset, internal errors can occur that may result in the new proxy settings not being used for all connections, or the old proxy settings continuing to be used. The workaround is to reboot the system after modifying the **Proxy Settings**.
KTS-3875	**LoadMaster HA Pairs:** When adding a device, if any LoadMaster HA pairs are expanded in the left frame, they close while the **Add a Device** screen is open and expand again once you click **Apply**. This is a cosmetic issue only.
KTS-3857	**LoadMaster HA Pairs**: In the Log Viewer, the Virtual Service and Real Server search boxes do not display Virtual Services and Real Servers for the HA nodes. The workaround is to use the **Text** search box instead.
KTS-3844 **KTS-4252**	If a Virtual Service uses a wildcard (*****) IP address, you cannot add Real Servers to the Virtual Service from KEMP 360 Central. The workaround is to add them using the LoadMaster UI; they are then displayed in the KEMP 360 Central UI.
KTS-3837	**LoadMaster HA Pairs:** If the shared IP address for a LoadMaster HA pair cannot be contacted, both HA units show their status as "Standby". You must restore access to the shared IP address from KEMP 360 Central to correct this issue. Possible causes are that the network of the shared IP address is unreachable or that the authentication parameters on one or both of the HA units in the pair was modified on the LoadMaster without making the same modifications on KEMP 360 Central.
KTS-3814	**LoadMaster HA Pairs:** If the two HA devices in a LoadMaster HA pair take significantly different times to poll (for example, HA1 takes one second, HA2 takes 10 seconds), the UI may report inconsistent data for up to one minute, until the next device status poll occurs.
KTS-3812	**LoadMaster HA Pairs:** When setting up Role Based Access Control (RBAC) for a user on LoadMasters configured in HA mode, ensure to assign the same level of access to all three devices in the LoadMaster HA pair; the HA1 device, the HA2 device, and the shared IP device.
KTS-3721	**LoadMaster HA Pairs:** If a LoadMaster HA unit configured in a LoadMaster HA pair is moved to "standalone" mode in the LoadMaster WUI, the effect on status reporting for that device in the KEMP 360 Central UI depends on the LoadMaster Operating System (LMOS) release: ●If the now standalone mode device is running on LMOS release 7.2.37 or later, that unit's device in KEMP 360 Central always shows as "down" in the KEMP 360 Central UI. ●If the now standalone mode device is running an LMOS release earlier than 7.2.37, the unit always shows its HA status as "Standby", even when it is

	"Active". The only indication you get that there is a problem is that the now standalone unit will never assume the "Active" role, even when the other unit is unavailable.
KTS-3438	In the log viewer, it is possible for the user to miss-configure a **Time Range** (for example, set a **From** date later than a **To** date), and then select another range (for example, **Last Week**). If the user then tries to export the log display, the export fails because the invalid **From** and **To** dates are still checked, even though they do not apply to the **Last Week** selection.
KTS-3427	Errors can occur when selecting multiple devices in the **System Reboot**, **Templates**, **Update LoadMaster Firmware**, and **Backup/Restore** menus in the **System Configuration** tab at the network level. If you experience these errors, use the **System Configuration** tab at the device level instead.
KTS-3390	When Amazon Web Services (AWS) Elastic Load Balancing (ELB) devices are present in the configuration, it is possible for status information for all devices to be delayed. Status information is processed and visible in the UI on a two-minute cycle, instead of every minute.
KTS-3304	If you create a user, give it full write permissions, and add it as a member of a custom user group - any device that user adds is not visible to that user in the network tree. The workaround is to specifically add the new device to the custom group.
KTS-2720	The **HTTP Method** field displays a blank value for HTTP/S health checks.
KTS-2707	Configuring a Layer 7 specific parameter on a Layer 4 Virtual Service should both enable Layer 7 services on the Virtual Service and set the new parameter value. Instead, only Layer 7 is enabled; the Layer 7 specific parameter is not set to the value specified.
KTS-2145	When using the **VS Motion Migrate** function, the virtual IP address and port for the new Virtual Service is not automatically updated when you select a LoadMaster from the **Target** drop-down list. You must update the address manually to an available IP address on a network accessible to the target LoadMaster.
KTS-2101	Setting the alternate IP address does not work on UDP services.

2.4 Known Issues with Specific LoadMaster Releases

The following table lists all issues in KEMP 360 Central that occur only with specific LoadMaster releases. If there is a fix for the issue, the release containing the fix is listed in the description.

ID	Description

PD-10051	**Local License Activations:** When re-activating a previously activated LoadMaster, it is not possible to choose a license on the LoadMaster that is above the previously-selected license in the menu. This issue is addressed in LoadMaster Operating System (LMOS) version 7.2.41.
PD-9947	Issues with Virtual Service status returns from LoadMasters running version 7.1.35.4 can result in incorrect Virtual Service health statuses being displayed in the KEMP 360 Central UI. This can occur when either Virtual Service status is requested from the LoadMaster, or when the Virtual Service is modified (if the issue is not already present). In the latter case, the issue should correct itself on the next UI status update (within a minute).
PD-9747	When monitoring two LoadMasters that are configured in an HA pair, and certificate authentication is in use, it is possible for KEMP 360 Central to lose contact with the standby (passive) LoadMaster. The recommended workaround is to reboot the standby LoadMaster. This has no effect on traffic through the HA pair (because this is the standby unit) and certificate-based authentication with KEMP 360 Central should be restored after the reboot. An alternative workaround is to edit the LoadMaster HA devices on KEMP 360 Central and switch the authentication setting from certificate to basic authentication. This issue is addressed in the 7.1.35.4 and 7.2.40 LoadMaster releases.
PD-9383 **PD-9398**	Most special characters supported in LoadMaster passwords are supported in V1.15 and later releases of KEMP 360 Central. However, because of an issue in the LoadMaster Application Program Interface (API), quotes and spaces in LoadMaster passwords can cause authentication from KEMP 360 Central to fail. However, they work without issue when logging directly into the LoadMaster WUI. As a workaround, you should log into the LoadMaster and update the password for the login that you supply to KEMP 360 Central so that it does not contain any spaces or quotes. Then, add the device to KEMP 360 Central. This issue is addressed in the 7.1.35.4 and 7.2.40 LoadMaster releases.

3 Version 1.26

Version 1.26 of KEMP 360 Central was released in August 2018 and was a feature and bug-fix release. It contains the new features, resolved issues, and known issues described in the following subsections.

3.1 New Features

Enhancements to Disk Storage and Database Resiliency

Enhancements have been made to improve visibility and control over disk space consumption in KEMP 360 Central, as well as reduce the system's disk footprint by default:

- Users will be able to control the statistics retention policy, which defaults to 3 months. Statistics older than the policy setting will be deleted.
- A separate log retention policy is also user-configurable and set by default to 3 months of logs for all managed devices.
- The default log message level configured on newly-added managed devices has been changed from INFO to ERROR, to reduce log pressure on disk space. This can be overridden by the administrator using existing controls on managed devices. The log level for existing devices on upgrade will not be modified.
- A new global parameter controls the log level accepted on receipt of logs from a managed device. If a message is received at a log level lower than the KEMP 360 Central global setting, it is dropped and not added to the log history. So, for example: if a LoadMaster is set to send INFO logs and above to Central, and Central's global setting is set to ERROR, then all messages received from the LoadMaster below the ERROR level are be dropped. By default, this behavior is Disabled – all logs received are stored.
- A disk space alert threshold has been added to configure the consumption level at which alerts will begin to be displayed to the user in the UI, emailed to the SMPT settings recipient list, and sent to the system log. The intent is to give the user notice that there is a potential disk space issue, and they can manage the above settings to set limits – or engage support for help before disk space consumption reaches critical levels. Alerts are provided on a per-partition basis on two-partition systems: one for the OS partition and one for the Data partition (which contains logs and statistics).
- Internally, a 'high water mark' of disk space consumption on the OS (or a single) partition has been defined at 95% -- the intent of which is to prevent disk space consumption from reaching a level that would make the system unresponsive. Once consumption reaches this level, all remote log collection stops until disk space is freed. As above, the intent is to allow the user to make use of the new controls provided and/or call support for assistance.
- All the above-mentioned controls are presented on a new **Settings and Configuration > Storage** accordion.

UI Session Limiting

An internal inactivity timer has been added to limit UI sessions to 24 hours. After 23 hours and 50 minutes of inactivity, a dialog is displayed to warn the user that their session is about to be closed, presents a 10-minute timer, and allows the user to continue or close their session. After the 10-minute timer expires, the session is terminated and the user is redirected to the login page.

3.2 Issues Resolved

ID	Description
KTS-5020	Addressed an issue with device statistics seen when a LoadMaster in an HA pair when it changes state from Master to Standby mode and then very quickly changes back to Master mode.
KTS-4964	Fixed an issue where the KEMP 360 Central UI does not return an error when an attempt to configure a new syslog target on a LoadMaster fails because the LoadMaster has already reached its limit on the total number of syslog targets allowed.
KTS-4279	When a user with read permission on the system configuration opens the System Settings page, a spurious error message is displayed that the user cannot perform the specified action. This issue has been fixed.
KTS-3999	Fixed an issue where specifying multiple email addresses for the Bcc: list on the SMTP Settings screen results in email being sent to only the first email address specified.
KTS-3820	In multiple locations in the UI, drop-down or combo box controls are used to present lists that can only be manipulated with the mouse or other pointing device only. These controls have been enhanced to also support keyboard navigation and selection.
KTS-2862	Fixed an issue where selecting a resource from the repository on Central (such as a backup, template, or firmware image), the UI only displays the most recent 20 items in the repository. Now, all existing resource are displayed.

4 Version 1.25.2

Version 1.25.2 of KEMP 360 Central was released in August 2018 and was a feature and bug-fix release. It contains the new features, resolved issues, and known issues described in the following subsections.

4.1 New Features

Increased minimum CPU, RAM, and Disk Requirements

The minimum system requirements for new deployments have been increased to the following:

Resource	Requirement
CPU	4 cores
RAM	8 GB
Disk storage	250 GB

For more information, refer to the **Virtual Machine Requirements** section.

4.2 Issues Resolved

The following are the major issues observed in previous releases that are resolved in this release.

ID	Description
KTS-5057	Upgrade: Fixed upgrade performance issues that could have expanded upgrade time to 40 minutes or longer.
KTS-5020	Statistics: Addressed in an issue observed with incoming LoadMaster statistics, where the data received during a LoadMaster High Availability (HA) failover event could be invalid.

5 Version 1.25

Version 1.25 of KEMP 360 Central was released in July 2018 and is a feature and bug-fix release. It contains the new features, resolved issues, and known issues described in the following subsections.

5.1 New Features

Central HA Support in MELA Deployments

Configuring two KEMP 360 Central units into a High Availability (HA) configuration is now supported in MELA deployments. For important configuration instructions and limitations, please see the **HA Configuration** section of the Kemp 360 Central Feature Description.

Disk Space Consumption Alerts

The alert mechanism has been enhanced to provide alerts when disk space consumption reaches 80% of the available disk space. An email alert will be sent to all configured email recipients (**Settings and Configuration > System Settings > SMTP Settings**) and a message is displayed in the UI banner at the top. When this alert is displayed, it is vital that you contact KEMP support to resolve possible disk space issues. Additional capabilities around disk space consumption issues will be provided in future releases.

UI Rendering on Smaller Screen Sizes

The KEMP 360 Central UI has been updated to maintain a static screen layout below the recommended viewing width of 1366 pixels wide. A horizontal scrollbar will appear below this width and all screen elements will maintain their appearance and relative placement.

Turning Off the Licensing Blacklist

In V1.23, a licensing blacklist capability was added to KEMP 360 Central that automatically deactivates licenses that have been activated by unauthorized LoadMasters. In this release, this mechanism has been enhanced as follows:

- The blacklisting feature is now off by default, on fresh installs and on upgrades. It can be enabled from the Settings and Configuration > System Settings page in the UI.
- When the blacklist is enabled, a list of devices that will disabled will be displayed on enabling the blacklist and when the admin user logs into the UI.
- The icon used for LoadMasters that have activated a license from Central but have not been authorized has been updated as shown below.

Old icon

New icon

5.2 Issues Resolved

ID	Description
KTS-4746	UI/UX: Fixed an issue that under certain circumstances could cause objects in the Network Tree to change position in the hierarchy when clicked.
KTS-4618	UI / UX: Fixed an issue that could cause an internal server error to occur after a firmware upgrade, requiring a hard reboot of the VM.
KTS-4530 KTS-4350 KTS-4349 KTS-3840	UI / UX: Addressed various issues with long nicknames causing display issues on multiple screens.
KTS-4518	UI / UX: Addressed issues in the dashboard where text in various widgets can be truncated causing misinterpretation of the data.
KTS-4516	UI / UX: Modified the way that 'down' Real Servers are counted on Central to mirror LoadMaster's behavior. Starting with the V1.25 release, if a Virtual Service is disabled, all Real Servers used by that service are also considered 'down' by Central. This results in, for example, the behaviour of counters of 'down' Real Servers in the Central UI dashboard now matching how 'down Real servers are counted in the LoadMaster WUI.
KTS-4410	Backup / Restore: Addressed issues seen restoring backup archives taken on Central units licensed for MELA where stub entries in the backed up database for reports that are not contained in the backup archive can cause Central to enter its licensing grace period.
KTS-4169	Open Source Software: Added version numbers for all software on the OSS software list found on the Help > About page.
KTS-3559	High Availability (HA): In previous releases, when a newly added managed device is added to one Central unit in an HA pair, the change is immediately communicated to the other unit -- but the

	receiving unit does not immediately poll the unit for configuration. The behaviour has been modified so that the 'new' managed device is immediately polled on the receiving Central instance, just as if it had been added to that instance.
KTS-3373	UI / UX: Fixed an issue where, if you attempt an operation that requires SMTP parameters to be set and they are not set, then multiple error messages are displayed by the UI. Instead, a single specific error message is now displayed.
KTS-3461	Security: Fixed an issue seen in previous releases on Azure where a single login created during the provisioning of the VM could be given administrative privileges.
KTS-2364	UI / UX / Upgrade: Addressed issues seen in previous releases after upgrade where the user's browser cache needs to be cleared before the UI is displayed properly.

6 Version 1.24

Version 1.24 of KEMP 360 Central was released in July 2018 and is a feature and bug-fix release. It contains the new features, resolved issues, and known issues described in the following subsections.

6.1 New Features

Device Up Email Notifications

KEMP 360 Central now provides email alerts when a device becomes available (i.e., goes 'up'), to complement the existing 'down' email alerts. The email is sent to the same list of recipients as 'down' emails, configured in the UI on the **Settings & Configuration > System Settings > SMTP Settings** page.

Monitoring Page Enhancements

KEMP 360 Central's **Monitoring** page now intelligently interprets the status of Redirect VSs and SubVSs as reported by LoadMaster so that the VS is regarded as available ('up') as long as the LoadMaster on which it resides is up and the Redirect VS is not specifically marked down (or otherwise unavailable) by LoadMaster. Additional enhancements were also made to provide nicknames and correct issues with SubVS IDs to improve the usability of the page.

Call Home

KEMP 360 Central has been enhanced to provide 'call home' functionality that reports various system configuration and statistical information to KEMP via the licensing server on a daily basis. This mirrors the similar LoadMaster 'call home' functionality. On initial deployment, the user will be prompted to choose whether to allow or disallow call home. On upgrade, call home will be disabled by default.

6.2 Issues Resolved

ID	Description
KTS-4568	Resolved an issue that caused a logout from the UI to occur when opening the same UI session in more than one browser tab.
KTS-4564	Fixed an issue where opening the Templates accordion at the network level did not display the version information for the listed templates.
KTS-4351	Fixed an issue that caused LoadMaster licensing information to be missing from the parent network display when only subnets in the parent network contained LoadMasters.
KTS-4337	Addressed performance issues that caused high resource usage

	and reduced response time when a large volume of managed device logs are being processed.
KTS-2693	Fixed an issue that prevented editing a service nickname.

7 Version 1.23

Version 1.23 of KEMP 360 Central was released in April 2018 and is a feature and bug-fix release. It contains the new features, resolved issues, and known issues described in the following subsections.

7.1 New Features

1. Availability Reporting

Central's Reporting UI (**Settings & Configuration > Reporting**) has been expanded to provide availability (up/down) history reports at various levels of granularity, for all devices or for a user-defined set of devices.

2. Monitoring Page Modifications

The general usability of the **Monitoring** page has been improved by making the following major updates, along with other minor updates:

- Providing the nickname for each object (VS, SubVS, Real Server) that has one, either on the screen or in a tooltip.
- Providing a better correspondence for SubVS index IDs between LoadMaster and Central.

3. Upgrade Logging Enhancement

To make troubleshooting easier, the upgrade process has been improved to provide more information in the system log with respect to both the upgrade process and status.

4. Enhanced ASL Licensing Management

In previous releases, it is possible for a MELA LoadMaster to activate an ASL license from Central, but without the device's credentials ever being added to Central so that the device can be managed by Central.

In this release, a timer has been added that specifies the amount of time that an unauthenticated ASL-activated device can remain in the Central configuration before it is automatically removed. The default is 3 days (72 hours). This default can be changed on the **Setting & Configuration > System Settings** screen.

When such a device is automatically removed, the admin user receives a notification and the device is added to an ASL blacklist. The device cannot get another license without first being removed from the blacklist. You can see such devices on the **Setting & Configuration > MELA Licensing Management** screen; they are listed in the table as BLOCKED and can be unblocked using controls on this page.

7.2 Issues Resolved

ID	Description
KTS-4569	Resolved an issue that caused a short delay between the time a network was deleted by the user and when it was actually removed from the network tree.
KTS-4561	In some scenarios, the **System Configuration > License** accordion doesn't open after clicking **View list** from the dashboard Licensing widget. This bug has been fixed.
KTS-4397	In previous releases, it is possible for an offline upgrade to fail if package dependencies in the upgrade cannot be resolved and KEMP 360 Central cannot access the internet to resolve them. This issue has been corrected: upgrades will not require internet access to resolve package dependencies.
KTS-4340	Fixed an issue where adding multiple AWS-ELB devices to Central can result in some of those devices being marked unavailable, when they are in fact available.
KTS-4297	Fixed an issue in the UI **System Configuration** tab that caused device nicknames to overlap with the device IP address in the tables presented on the various accordions on this page.
KTS-4261	Modified the process for changing a user password: after successfully changing the password on the account you used to log into Central, you are logged out of the system. You must then log in again using the newly set password.
KTS-4257	Fixed an issue that caused the **Metered Licensing Management > Automatic Reporting** UI to show a report failure when no report had yet been sent.
KTS-3850	Corrected issues seen in the field when restoring a backup taken on one member of a Central HA Pair to the other unit in the pair. Please note that, after the restore is complete, the HA configuration on the restored Central unit must be updated to point at the other HA unit.
KTS-3561	Fixed an issue in the Reporting UI that caused the last column in a 1-day report to be truncated.

8 Version 1.22

Version 1.22 of KEMP 360 Central was released in February 2018 and is a bug-fix release. It contains the resolved and known issues described in the following subsections.

8.1 Issues Resolved

ID	Description
KTS-4264	Fixed a problem displaying the device list on the system configuration page that occurs when HA pairs are present in the system and one of the HA devices is down.
KTS-4185	The 'total' statistics for WAF on the dashboard have been removed from the widget to provide better dashboard performance. These counts will be added back to the UI in a future release.
KTS-4135	In previous releases, it was not possible to remove a device from KEMP 360 Central unless Central could connect to the device using its API. Starting with V1.22, a device can be removed from Central regardless of whether Central can connect to the device.
KTS-4130	Fixed an issue with scheduled reports failing to adjust the displayed next run date for the browser's time zone, and instead displaying it in the UTC time zone.
KTS-4125	Added a tool tip to the system gauges in the Monitoring page for a single device to provide the actual traffic level on interfaces. This was done to address an issue where low levels of network traffic were not resulting in any visible output in the interface bar graph.
KTS-4120	Fixed an issue relating to the LoadMaster password field.
KTS-4116	Fixed an issue that might result in a negative number being displayed in the warning banner when the system time is changed.
KTS-4049	Fixed various issues associated with cleanup of old scheduled actions, non-repeating actions, and some actions being executed starting 'today' instead of the configured start date.
KTS-3878 KTS-4009	Made various changes to the UI and API to improve UI performance.

KTS-3525	Fixed an issue that in some cases caused re-activating a LoadMaster via ASL on KEMP 360 Central to fail when a different license is chosen than the current license.
KTS-3130	Fixed issues in the UI where unavailable devices or HA Shared IP devices could be selected for operations on the system configuration page that are not allowed on such devices.

9 Version 1.21

Version 1.21 of KEMP 360 Central was released in January 2018 and is a feature and bug-fix release. It contains the features, resolved issues, and known issues described in the following subsections.

9.1 New Features

Time and Date Configuration and Visibility

The **Settings and Configuration > Date and Time** UI allows you to:

- Configure up to 3 NTP servers to synchronize the system date and time. You can use an IP address, an FQDN, or the name of a public NTP time server (e.g., pool.ntp.org).
- Provide credentials to use with NTPv3 servers that require authentication.
- Manually set the date and time. Note that making manual changes to date and time is strongly discouraged due to the potential for negative consequences on system operation.

Also note the following:

- The time zone used in the UI is the same as that used by the client browser you are using to access the UI – which is usually set in the system setting for the device on which the browser is running.
- The current date, time, and time zone are displayed in the upper right corner of the KEMP 360 Central UI's blue banner.
- On upgrade and in a new deployment, NTP is enabled by default. The default NTP time server used is pool.ntp.org.
- On most UI screens, like Monitoring and Graphs, data is presented in the local time zone. The notable exception is the Repository > Logging page, which uses UTC to display logs from managed devices.
- On upgrade, existing scheduled actions will be unaffected and will continue to execute at the originally configured time.

9.2 Issues Resolved

ID	Description
KTS-3451	Fixed an issue where the devices.csv file in a downloaded MELA Report could not be opened due to a file type mismatch.
KTS-3413	Fixed an issue that caused an ASL activated unit to be unable to negotiate certificate authentication immediately upon being added, until the next hourly or manual configuration poll.
KTS-3197	Fixed an issue where killing an ASL activation from the

	LoadMaster side would not remove the device from the network tree on Central, because of a polling conflict.
KTS-3123	Fixed an issue where adding a LoadMaster to Central and then activating an ASL license from the newly added LoadMaster did not change the network tree icon for the device to a (blue) LoadMaster icon.

10 Version 1.20

Version 1.20 of KEMP 360 Central was released in December 2017 and is a bug-fix release. It contains the resolved and known issues described in the following subsections.

10.1 Issues Resolved

ID	Description
KTS-3981	Security: Updated the system Python component to address security vulnerabilities (CVE-2017-1000158 / USN-3496-3).
KTS-3905	UI/UX: Enhanced the performance of the Dashboard WAF Summary.
KTS-3859	AWS Platform: Updated system components to fix deployment issues in AWS.
KTS-3858	Reporting: Fixed an issue that caused the 'Event Type' column in MELA reports to break the layout of the ASL activations table.
KTS-3854	UI/UX: Fixed issues associated with improper display of network tree icons during a managed device reboot.
KTS-3839	UI/UX: Addressed issues with data display in the Dashboard WAF Summary.
KTS-3833	Azure Platform: Updated the system Azure Agent component to the latest release.
KTS-3819	UI/UX: Fixed issues associated with improper display of network tree icons during a reboot of the HA Shared IP device in a LoadMaster HA Pair.
KTS-3740	LoadMaster HA Pairs: Fixed validation issues in the LoadMaster HA Pair add screen when the same IP is chosen for HA1 and HA2.
KTS-3580	RBAC: Fixed an issue with permissions where a user with write access on system configuration but read access on service configuration can't perform any system configuration operation (such as rebooting a managed device).
KTS-3505	UI/UX: Returned UI functionality from previous releases where a 'Read-Only' indicator is included in the blue banner

	when a device to which the user has only read access is selected in the network tree.
KTS-3142	Reporting: Improved error returns and expanded the amount of information logged for reports for both success and failure conditions.
KTS-3141	Reporting and RBAC: Fixed an issue where the devices available for selection during report creation are filtered according to the user's permission settings.

11 Version 1.19

Version 1.19 of KEMP 360 Central was released in November 2017 and contains the new features, resolved issues, and known issues described in the following subsections.

11.1 New Features

Monitoring LoadMasters in HA Mode

A new device type, LoadMaster HA Pair, creates a relationship in Central between two LoadMasters that are configured into HA mode to provide high availability services. This allows you to more effectively monitor the status and configuration of services across the high availability pair.

For more information, see the **Appendix: Quick Start for Monitoring LoadMaster HA**.

Support Added for Multiple Devices with the Same IP Address, Unique Ports

In previous releases, a unique IP address must be specified on device creation, regardless of the port specified. With Version 1.19, you can now create a new device that uses the same IP address as an existing device, as long as you specify a unique port for the new device.

Upgrade UI Enhancement

The upgrade process has been updated to prevent the user from navigating away from the upgrade screen before the upgrade is complete and the system reboots. This will prevent issues seen in previous releases where navigating around the UI during the upgrade process could result in unexpected results.

Improved MELA Reports

The design of the printed reports for MELA deployments (Settings and Configuration > Metered Licensing Management) has been updated to provide better readability and an improved layout.

Support for KVM and Xen Hypervisors

A new system image is provided with this release that can be installed and run under either the KVM or Xen hypervisors. These new images support the full range of KEMP 360 Central features supported on current platforms.

11.2 Issues Resolved

ID	Description
KTS-3654	Fixed an issue that could cause scheduled actions to be executed at the wrong time, or not at all, depending on the difference between UTC and the local browser time when the action was scheduled.

KTS-3584 **KTS-3580**	New users with write permission on the system configuration cannot perform some actions, such as firmware upgrade, template upload, and backup. This issue has been fixed.
KTS-3578	The ASL Server has been enhanced to provide better audit and debug logging for ASL license activation and other ASL related events.
KTS-3568	Fixed an issue that caused a scheduled action that should have been performed once to be executed daily.
KTS-3566	Fixed an issue that could cause a scheduled action's status to go unrecorded.
KTS-3563	Reports are only delivered to the first recipient if multiple recipients are specified. This issue has been fixed.
KTS-3529	An internal status processing issue can result in Real Server status on F5 devices being updated only when there is a configuration update on the F5 unit. [This issue does not affect other 3rd party devices or LoadMaster.]
KTS-3502	Fixed an issue in the Application Health widgets where the displayed status is not being shown correctly for some period of time after a status change occurs.
KTS-3440	If invalid credentials are specified for a device, a critical-level message is written to the log and a corresponding email alert is sent every minute. This should only happen once, when the device goes from a previously authorized state to unauthorized. To work around this issue, edit the device definition on Central and supply the correct credentials for the device (or remove the device).
KTS-3381	When a manual configuration poll is requested from the Monitoring page of a device, two identical emails may be sent when a critical condition occurs (such as device going down). This issue has been fixed.
KTS-3344	Addressed an issue in Central that caused under-reporting of the WAF event statistics displayed in the Dashboard, when compared to the statistics seen in the LoadMaster WUI.

KTS-3331 **KTS-3153**	Under certain conditions, the Monitoring page displays gray-colored graphs with incoherent labels. This bug has been fixed.
KTS-3321	Fixed an issue that caused the copy or move of a Virtual Service (VS Motion Migrate) to a unit that is ASL-activated to fail.
KTS-3230	Improved Central's management of user logins created on LoadMaster, so that Central will never have more than one login for its use on LoadMaster.
KTS-3222	Enhanced the validation performed on the user-supplied SSH key file for xroot login to disallow a key that is not in the correct format.
KTS-2672	Setting Virtual Service persistence to 'none' from Central has no effect; the setting remains unchanged on LoadMaster. This bug has been fixed.
KTS-2646	Under certain circumstances, the Dashboard Connections widget does not display correct data. This bug has been fixed
KTS-2511	Central has been modified to no longer change the Message of the Day on a LoadMaster when it is added to Central.

34

12 Version 1.18

Version 1.18 of KEMP 360 Central was released in September 2017 and contains the new features, resolved issues, and known issues described in the following subsections.

12.1 New Features

ASL Personal Inventory

KEMP 360 Central has been enhanced to support the ASL Personal Inventory feature for LoadMasters that are licensed using the ASL Activation feature. This has several major impacts on activating a license from LoadMaster:

> When LoadMaster contacts Central to activate a license, Central sends a list of available licenses to LoadMaster so that the administrator can choose which license they want to use. LoadMasters can also re-activate and choose a different license than the one originally chosen.

> Central is no longer restricted to issuing licenses only to LoadMasters running on the same hypervisor platform. Licenses for LoadMasters running on any supported platform (VMware, Azure, AWS, etc.) can be activated from a single Central deployment, regardless of the platform on which Central is deployed.

> Central tracks activations directly and enforces licensing limits, so that there's no need for the LoadMaster to contact the KEMP licensing server directly.

Network Selection on Device First Contact

In previous releases, Central only performed automatic placement of a device into the network tree if it was added from the **Welcome** page and immediately contacted. This has the consequence that, if contact on addition is unsuccessful, the device is moved to the **Unmanaged Devices** node; at some later time, upon successful contact, it would be placed at the bottom of the network tree. The user would have to manually place the device into the network tree by editing the device and choosing from among matching networks, or creating a new network in which to place it.

In V1.18, automatic placement into a network is performed whenever a device is contacted for the first time, and regardless of whether it is added via the **Welcome** page or the add icon (+) at the bottom of the network tree.

Enhanced Cloud Public IP Address Support

Public IP address support for cloud ADCs has been enhanced to remove the possibility of the device being automatically re-added by KEMP 360 Central using the device's internal IP address.

Enhanced Error Handling for Certificate Authentication

Certificate Authentication negotiation has been enhanced to handle connection errors as well as HTTP errors. Connection errors are now returned to the user and logged to improve the ability to troubleshoot connectivity issues when setting up certificate authentication.

Manual Configuration Update for 3rd-Party Devices

The ability to manually request a configuration update for a device has been extended to non-LoadMaster devices (F5, NGINX, AWS, HAproxy). The button to request an update appears on the Monitoring tab for these devices. Note that, for LoadMasters, the button has been moved from the System Configuration tab to the Monitoring tab, to be consistent across all device types.

12.2 Issues Resolved

ID	Description
KTS-3443	Fixed an issue that caused modifying both the IP and port of a device at the same time to fail.
KTS-3433	Fixed issues displaying the Open Source Licensing page in the UI.
KTS-3429	Creating a new one-time scheduled action (selecting 'Never' for the 'Repeat' parameter) returns an error complaining that a required parameter is not set. This issue has been fixed.
KTS-3426	Modified the dashboard Device Health and Log Summary widgets to more clearly indicate the at-a-glance status.
KTS-3398	When upgrading to V1.17 or a later version from a version prior to V1.17, licensing information for LoadMasters will not display the Time Zone with the license dates. This will cause the licensing widget to not contain any data directly after the upgrade and will also cause licensing information displayed on the System Configuration tab to be displayed without any time zone. This issue has been fixed.
KTS-3389	Moving or copying a service from one LoadMaster to another using KEMP 360 Central can fail if the target LoadMaster is using basic authentication and the source LoadMaster is using certificate authentication. This issue has been fixed.

ID	Description
KTS-3307	If you configure SMTP settings to use a 'Connection Security' setting of 'None', click the Send Test Email' button, and then the connection test fails -- you may be unable to change the 'Connection Security' setting afterwards. This issue has been fixed.
KTS-3153	Fixed issues that caused graphs to be rendered without color (i.e., in gray).
KTS-3121	If a device under the 'Unmanaged Devices' node is edited and saved, and the device cannot be contacted directly after editing, this can cause the unmanaged device to be moved to the bottom of the network tree, and the icon to change to a 'down' (red) icon, instead of the unmanaged device icon. This issue has been fixed.
KTS-2935	Fixed issues that caused some default LoadMaster VS options to be displayed incorrectly on Central.
KTS-2896	Fixed API issues that caused a non-admin user to be automatically added to a custom group.
KTS-1900	Fixed an issue where setting a health check URL with query parameters did not synchronize properly to LoadMaster.
KTS-1825	Fixed issues associated with being unable to delete custom headers in a health check. This issue is fixed for all LoadMaster releases 7.1.35.4 and above.
KTS-1814	Fixed an issue where adding a UDP protocol VS from Central resulted in spurious errors (the VS was created on the target LoadMaster).

13 Version 1.17

Version 1.17 of KEMP 360 Central was released in August 2017 and contains the new features, resolved issues, and known issues described in the following subsections.

13.1 New Features

LoadMaster Authentication Options

The **Add Device** and **Edit Device** forms for LoadMaster have been enhanced to include a new setting for **Authentication**. By default, KEMP 360 Central will try to negotiate certificate authentication for those LoadMasters that support it. Starting with this release, you can now edit the **Authentication** setting so that the unit uses basic authentication and does not attempt to establish certificate authentication.

Please note that certificate authentication is available in LoadMaster OS releases 7.1.35 and above; earlier releases can only use basic authentication. If a LoadMaster is running 7.1.34 or below, you will not be able to set certificate authentication for that LoadMaster.

Adding 3rd Party Devices on the First Time Login / Welcome Screen

The **About & Help > Welcome on Board** screen – which is also displayed on first time login to the device -- has been enhanced to allow addition of any third-party device type (AWS ELB, F5, HAproxy, NGINX), in addition to LoadMaster.

Graphs Moved from Monitoring Page to New Graphs Page

With many devices and/or virtual services, the **Monitoring** page in previous releases could become cluttered and long due to the amount of data being displayed. To address this issue, the graphs formerly displayed at the bottom of the **Monitoring** page have been moved to a new **Graphs** tab. In addition, all three graphs now use the same horizontal width/scale so that time-based comparisons between the graph data are easier to visualize.

Performance Enhancements

Various internal subsystems have been modified to improve the responsiveness of the UI and the overall performance of KEMP 360 Central. As a consequence of these changes, KEMP 360 Central is now capable of hosting a maximum of 150 managed devices and 2850 resources them (Virtual Services, SubVSs, and Real Servers). This is double the recommended maximum capacity in the V1.14 release.

Part of the performance work involved splitting the mechanisms used to gather status and configuration changes from managed devices into two asynchronous cycles:

- **Availability status** of managed devices and the load balancing objects defined on them (Virtual Services, SubVSs, and Real Servers) is updated every minute.
- **Configuration status** of managed devices and the objects defined on them is updated every 60 minutes. Please note the following:

- If the configuration change is made from KEMP 360 Central, the change is reflected immediately in the KEMP 360 Central UI.
- For LoadMaster devices, you can also request an immediate configuration update using the **Request Update** button found on the LoadMaster's **System Configuration** tab. [This functionality will be made available for third-party devices in a future release.]

13.2 Issues Resolved

ID	Description
KTS-3405	Closed a security vulnerability (CVE-2016-9877) that could allow a malicious user to obtain unauthorized access.
KTS-3310 KTS-3313	Issues with icon rendering in multiple release of Safari and text box rendering in Safari 9.1 have been resolved.
KTS-3259	Fixed an issue with uploading templates to a LoadMaster where the cancel button on the confirm dialog did not cancel the action.
KTS-3228	Fixed issues with certificate authentication caused by a mismatch of the character set used between KEMP 360 Central and LoadMaster.
KTS-3182	Addressed an issue in the Reporting interface where no data point was plotted on graphs if no data was collected, while '0' was reported in the accompanying tables. Now, graphs will also display a data point of '0'.
KTS-3128	Fixed various issues with certificate authentication to LoadMasters. Note that addressing some of these issues will require upgrading LoadMaster to either the latest LTS image (7.1.35.4 available in August) or 7.2.40 (available in October).
KTS-3103	Fixed various errors with Metered Licensing (MELA) deployments: • MELA report contains errors and no data. • Discrepancies between the printed and emailed MELA report data. • Issues with re-trying the MELA report upload. • The 'grace period' for MELA units not contacting KEMP does not get reset at appropriate times. • MELA reports show device numbers with no way of connecting report data to customer devices. • MELA report for two consecutive months contains duplicate data. • Response from KEMP licensing server causes unexpected

ID	Description
	errors.
KTS-3091	Fixed an issue in the network tree where sub-networks did not sort correctly within the containing network.
KTS-3067	Added to the About & Help > About page a link to display licenses for all the Open Source Software (OSS) incorporated into KEMP 360 Central.
KTS-3037	Fixed an issue in the System Configuration pages where enabled check boxes stay selected even after an operation (e.g., a backup) has been completed. Check boxes are now returned to their default state after completion.
KTS-3021	Fixed an issue that prevented SPLA-enabled images of LoadMaster with 'unlimited' licenses from being added to KEMP 360 Central.
KTS-3020	Fixed an issue that prevented adding a LoadMaster in certain situations where multiple network interfaces were defined on the LoadMaster, but not all of them were configured.
KTS-3000	Moved MELA reports from temporary storage to another location to address MELA reporting errors. On upgrade, messages like the following will be received, one for each report that has been moved: CRITICAL A scheduled report has been identified that will no longer run successfully, because the report data no longer exists. This report has been removed from the system: Usage Report for KEMP 360 Central v1.14.0.1536 May 2017 SN xxxxxxxxxx If you experience any issues with MELA reporting, please contact KEMP support and include these messages in your communication. Otherwise, these messages can be ignored.
KTS-2773	Added a confirmation step to various System Configuration operations (e.g., backup and restore) before beginning the operation.
KTS-2705	Fixed a possible security issue with logins, where and a user with 'write' permission could change the admin user's credentials.
KTS-2456	Fixed an issue that caused third-party security scanning tools to report that MySQL accounts on KEMP 360 Central were configured

ID	Description
	insecurely.

14 Version 1.15

Version 1.15 of KEMP 360 Central was released in May 2017 and contains the new features, resolved issues, and known issues described in the following subsections.

14.1 New Features

Device Assessment Reports

The new **Settings and Configuration > Reporting** page allows you to print ad-hoc and scheduled reports for selected devices. The reports contain a graphic and tabular summary of the devices' performance over the time period selected for the report.

The report is created as a PDF file and can either be downloaded directly or sent via email to a specified list of recipients.

Previously scheduled reports are tracked in the UI and can be modified.

Unmanaged Devices Node

In previous releases, devices added to KEMP 360 Central that could not be successfully contacted were added to the bottom of the network tree, outside of any network. A new node to contain these devices, name **Unmanaged Devices**, now appears at the top of the network tree. If there are no unmanaged devices, the node does not appear.

Once KEMP 360 Central successfully logs into an unmanaged device, it is moved out of the **Unmanaged Devices** node and placed in the appropriate network based on its IP address.

Device Icon Legend

A legend describing all the icons used in the network tree has been added to the bottom of the left frame, to the right of the controls uses to add, delete, and edit networks and devices.

14.2 Issues Resolved

ID	Description
Various	Made a number of minor updates throughout the UI to improve usability and consistency.
KTS-1558	Fixed issues that prevented adding a LoadMaster with a password containing special characters (e.g. "#").
KTS-2552	Fixed issues in the MELA management UI where a report date in the future could be selected, resulting in an error when a report is created.

KEMP 360 Central Release Notes

ID	Description
KTS-2927	Fixed issues observed displaying the Dashboard with a reduced screen width.
KTS-2928	The Tiered Subscription UI has been enhanced to allow the user to sort the table of licenses by either IP Address (default) or Expiration Date. Only data for active LoadMasters is displayed; if the LoadMaster is down or has never been contacted, no licensing information is displayed for that unit.
KTS-2992	Upgrading the KEMP 360 Central firmware can no longer be performed by downloading an online image using the UI. The online upgrade option has been removed from the Firmware Management page. Instead, download the image from the KEMP Support Site to your local system and use the Firmware Management controls to upload the image to KEMP 360 Central for installation. The table will be updated automatically as device availability changes over time.
KTS-3015	Fixed a timeout issue where a newly added LoadMaster can be erroneously marked as unreachable when it is first added, even though the device is available and responsive.
KTS-3016 KTS-3019	Fixed issues where a failure to retrieve licensing information from a LoadMaster would result in that LoadMaster being treated as down by KEMP 360 Central.
KTS-3017	Fixed an issue that resulted in basic authentication credentials being included in debug log messages.

15 Version 1.14

Version 1.14 of KEMP 360 Central was released in March 2017 and contains the new features, resolved issues, and known issues described in the following subsections.

15.1 LMOS Version Support

With Version 1.14, KEMP360 Central officially supports managing LoadMasters running LMOS Version 7.1.34, or a later release. Earlier releases can still be managed with KEMP360 Central, but for full support you should upgrade to at least Version 7.1.34. Note that older LMOS releases will experience the following operational limitations:

- LMOS releases prior to 7.1.34 do not report network interface information & statistics. Because of these and other limitations present in LMOS, KEMP360 Central will perform optimally in a configuration of 50 devices or fewer running releases prior to 7.1.34.
- In addition, LMOS releases prior to 7.1.30b report fewer overall statistics.

15.2 System Sizing Limitations

In general, KEMP360 Central version 1.14 will work optimally with a configuration of up to 75 managed devices (whether they are LoadMaster or third-party ADCs, or a mix). The maximum number of managed devices that can be monitored with good UI performance also depends on the number of underlying resources (Virtual Services, SubVSs, and Real Servers) being monitored on each ADC, which is limited in this release to up to 1425 resources total across all managed devices. If concurrent users log in to KEMP360 Central, system performance will be affected and users will see increased rendering times in the UI. System scalability will be improved in subsequent releases.

The above limitations assume that all LoadMasters are running version 7.1.35 of the LMOS software, or a later version. See the section **LMOS Version Support**.

15.3 New Features

KEMP 360 Central High Availability

Version 1.14 contains a beta release of High Availability (HA) for KEMP 360 Central. With this release, the following functionality is provided:

- Two instances of KEMP 360 Central can be configured into an HA pair, using the controls located under **Settings and Configuration > HA Configuration** in the user interface. [If you are using Metered / ASL Licensing, please contact KEMP to discuss HA support.]
- With respect to failover, the two KEMP360 Central HA instances participate in a Master/Slave relationship:

- One system is designated the Preferred Master unit, and this unit should be configured first. Whatever configuration exists on this unit when it is configured into HA mode will be propagated to the other unit (the Preferred Slave).
  - If the Preferred Master unit becomes unavailable, the Slave unit assumes the Master role.
  - Once the Preferred Master is available again, it will automatically re-assume the Master role (i.e., fail-back to the Master role, and the other unit will assume the Slave role again).

- With respect to the data managed by KEMP360 central, the two units cooperate as follows:

  - Configuration changes made on either KEMP360 Central instance are reflected in the configuration and communicated to the other host.
  - Both of the KEMP360 HA instances collect system logs from managed devices. Therefore, each LoadMaster in the configuration will have both KEMP360 Central HA units as syslog targets.
  - Only the Master unit collects and generates statistics; the Master unit periodically forwards statistics to the Slave unit.

> Please note that when configuring two KEMP360 Central instances into HA mode in this release, both units need to have at least one network defined for the initial synchronization to complete successfully.

> Remember: Once the two units are initialized into HA mode, the configuration of the Preferred Master will be propagated to the Preferred Slave, and the Preferred Slave's configuration will be overwritten. After initial synchronization has completed changes will be propagated in both directions.

LoadMaster Licensing & Tiered Subscriptions Summary

KEMP360 Central has been updated to provide a summary of LoadMaster traditional and tiered subscription licensing, so that KEMP360 Central administrators can quickly identify LoadMasters that are approaching or have passed a license-related expiration date.

A new Global Dashboard application, **Non-Local Licenses and Subscriptions**, reports the number of LoadMasters that have licenses or subscriptions that have expired or that are about to expire in 7, 30, or 60 days. These LoadMasters have been licensed using either legacy licenses or the latest tiered subscription based licenses. [Note: licenses activated via the KEMP360 Central Activation Server Local (ASL) feature are reported in a separate Local Licensing dashboard application.]

Clicking on N**on-Local Licenses and Subscriptions** opens a new **Licensing** table on the **All Networks > System Configuration** page. This table lists the IP Address, Name, License or Subscription, and Expiration date for all managed LoadMasters. If a license or subscription is expired, it is displayed in red text.

LoadMasters with legacy licenses will have one entry in the table. LoadMasters licensed with tiered subscription based licenses will have one entry for the license type (Standard, Enterprise, or Enterprise +) and additional entries for each subscription.

15.4 Issues Resolved

ID	Description
Various	Improved UI performance through a number of internal changes. See **System Sizing Limitations** for sizing recommendations for best UI performance.
KTS-2942	Improved usability of the default state of the backup and restore configuration page.
KTS-2936	Fixed an issue in System Configuration where choosing Rebooting Selected reboots all devices instead.
KTS-2930 KTS-2155	Fixed issues that caused the Monitoring page network traffic graphs to display larger values than expected, either in the graph or in the tooltips for specific data points.
KTS-2906	Improved usability of the UI by displaying a progress bar when a large amount of data is being loaded.
KTS-2849	Fixed a configuration issue that occurred when setting the persistence method to none.
KTS-2848	Fixed an issue in the UI Monitoring page where, in large configurations, messages reporting LoadMasters coming online repeatedly appear.
KTS-2772	Fixed a UI issue where clicking the Reboot All button in the UI did not reboot any devices.
KTS-2771	Fixed UI rendering issues when listing templates with long names.
KTS-2685	Fixed an issue in the Add a Device page where the Network field is not properly pre-populated with the currently selected network.
KTS-2670	Fixed a UI issue where clicking the Delete SubVS button does not delete the SubVS.
KTS-2150	Modified the date format used in various graphs and tables found under Settings and Configuration > Metered Licensing

ID	Description
	Management to consistently use the Year-Month-Day format.
KTS-1907	SSL TPS and Connections graphs under certain circumstances display a -1 value on the Y-axis, instead of or below the 0 value.

16 Version 1.12

Version 1.12 of KEMP 360 Central was released in January 2017 and contains the new features, resolved issues, and known issues described in the following subsections.

16.1 New Features

Log Viewer Enhancements

Click the **Global Repository** icon at the bottom-left corner of the UI to display the **Logging** page. From this page, you can search all the logs collected from all the devices that are managed by KEMP 360 and have been configured to send logs to KEMP 360. [LoadMaster, F5, NGINX, and HAProxy devices all support remote syslog; LoadMaster is configured automatically from KEMP 360 while the other devices must be configured manually.]

On the left, the time period for the log search can be set. Controls at right allow you to filter the logs for the selected time period by several new criteria:

- **Text:** Type in a simple text string (this was the only criteria supported in the previous release).
- **Log Severity:** Use the slider control to range of log message severities that you want to see in the search results.
- **Device IP:** To filter for a single IP address, select from a list of IP addresses for all devices managed by KEMP 360. The IP addresses are organized by device type (LoadMaster, F5, NGINX, HAProxy) then by IP address. If you select a device type, then only entries from all devices of that type will be searched (e.g., all LoadMasters or all F5 devices).
- **Virtual Service IP:** Select from a list of IP addresses for all virtual services managed by KEMP 360.
- **Real Server IP:** Select from a list of IP addresses for all real servers managed by KEMP 360.

Global Dashboard

A new global dashboard is added that displays key information such as device, infrastructure and application health in separate panes with clear indicators. The data presented includes:

- Device Health
- Top 3 utilization
- Local License Allocation
- Log Summary
- Virtual Service Status
- Real Server Status
- Administratively Disabled Services and Servers
- WAF Statistics Summary
- Active Connections Summary

First Time User Login Experience Improvements

When logging into a newly deployed KEMP 360, the system now prompts you automatically to add your first LoadMaster device. You can add one or more LoadMasters, optionally populating the KEMP 360 Central SMTP (email) parameters from the LoadMaster being added.

Add Device Workflow and Network Tree Organization

The workflow for adding any device (LoadMasters and 3rd-party devices) now locates your device by default in the network with the smallest address space that contains the IP address you specified for the device. If the device cannot be successfully contacted upon adding it to KEMP 360, the device is located at the bottom of the network tree, and will be moved to its appropriate location in the tree once the unit has been contacted and its configuration read by KEMP 360.

After the device is added, the default device location in the network hierarchy can be changed by the administrator by editing the device configuration. The device will remain in that location until the administrator specifically modifies it.

KEMP 360 Backup and Restore

Click the **Settings and Configuration** icon at the bottom-left corner of the UI and then click **Backup & Restore** to display the **Backup** and **Restore** control panes. The backup archive created contains a complete copy of the current running configuration, including all managed devices, services, networks, and KEMP 360 settings. The backup archive is encrypted and password-protected, and is saved locally to the system from which you launched the KEMP 360 Central user interface.

Similarly, the restore facility allows you to upload a previously created KEMP 360 backup archive from your local system and overwrite the current KEMP 360 configuration using the information in the archive.

The backup and restore facility is intended for disaster recovery – the device on which a backup archive is restored is expected to be equivalent to the device on which the archive was created with respect to network configuration and licensing. Other restrictions apply to restore operations when:

- Restoring an archive created on a unit other than the one on which the archive was created.
- Restoring an archive to a newly provisioned device while the device on which the archive was created is still active.
- Restoring an archive that employs local licensing from a KEMP 360 ASL Activation Server.

For more information, see the backup and restore documentation in the **KEMP 360 Central Feature Description**.

16.2 Issues Resolved

ID	Description
KTS-2721	Fixed an issue where requesting status from a LoadMaster

	running a release prior to 7.1.32 causes KEMP 360 to stop requesting status from all devices.
KTS-2700	Fixed an issue with graphs where a device becomes unavailable, but related graphs continue to display the last data values received from the device.
KTS-2677	Fixed an issue displaying multiple subnetworks on network Monitoring pages.
KTS-2664	Fixed a shell command injection issue in the UI.
KTS-2549 KTS-1496	Fixed an issue that caused the graph of locally licensed LoadMasters in the MELA report to omit valid activations.
KTS-2490	Fixed an issue with VS Motion where KEMP 360 returns an error message even though copying the virtual service succeeded.
KTS-2489	Fixed an issue where a LoadMaster is successfully added to KEMP 360 but its virtual services are not instantiated.
KTS-2488	Fixed an issue with access control groups where adding a group member resets group resources.
KTS-2487	Fixed an issue where editing permission group details failed under certain circumstances.
KTS-2486	Fixed an issue where adding, editing, or deleting a service or real server appears to succeed, but actually fails and causes the target LoadMaster to become inaccessible from KEMP 360.
KTS-2453	Fixed an issue where editing a Real Server port instead adds another Real Server to the system, and the existing server is disabled.
KTS-2383	Fixed a problem with VS motion where the user is unable to edit the VS alternate address before copying the VS, possibly resulting in duplicate IP addresses on the target unit.
KTS-2229	Several issues related to wildcard ports on Virtual Services were present in previous releases: • A wildcard port specified when adding or modifying a VS returned an error. • An existing VS on a LoadMaster added to KEMP 360 would not be instantiated on KEMP 360.

	•These issues have been fixed.
KTS-2004	Fixed an API issue where deleting a network without specifying an ID deletes all networks within the system.
KTS-1997	In previous releases, when editing an Access Control user group, the tree of resources (managed devices and services) displayed in the Edit Group pane shows the IP address of the resource. In this release, the display now shows the resource Nickname, if one exists; otherwise, it displays the resource IP address.
KTS-1860	Usability: Modified the default scheduling period for rebooting a device from 'Daily' to 'None'.
KTS-1823	The UI-has been enhanced to include persistence in the settings for UDP protocol virtual services.

17 Version 1.9

Refer to the sections below for details about the KEMP 360 Central version 1.9 features. Version 1.9 was released on 29th September 2016.

17.1 New Features

1. **Local Authorization and User Access**

This enables KEMP 360 Central users to be created with specific permissions to enable access to device management functions. Users can further be added to groups to aid control and access to the available device management functionality.

2. **Log Rendering**

There is a new log display and filter functionality available in the KEMP 360 Central User Interface (UI).

3. **F5 BIG-IP Support**

It is now possible to add/edit/remove F5 BIG-IP devices and visualize key traffic metrics and statistics from within the KEMP 360 Central UI.

17.2 Feature Enhancement

1. Virtual Service heat maps have been removed.

17.3 Issues Resolved

ID	Description
KTS-1877	Fixed a UI issue where some input fields were not displaying correctly in Firefox.
KTS-1875	Fixed an issue that was preventing the menus from expanding on the Welcome on Board screen on some occasions.
KTS-2001	Fixed an issue with hover text on Firefox.
KTS-1980	Fixed an issue that was preventing a Virtual Service with a Real Server from being deleted after a second Virtual Service was added.
KTS-1973	Fixed an issue relating to the LoadMaster password field.

KTS-1933	Fixed an issue that was preventing a network from being deleted if LoadMasters and Virtual Services were present in that network.
KTS-1920	Fixed a synchronization issue between KEMP 360 Central and LoadMasters relating to health checks.
KTS-1836	Added a progress bar to the initial licensing screen.
KTS-1809	Fixed an issue that was causing the spinner to appear indefinitely after clicking the Apply button when editing the SMTP settings.
KTS-1561	Fixed an Application Program Interface (API) issue relating to editing reports.
KTS-1465	Made improvements to the user change password field behavior.

18 Version 1.8

Refer to the sections below for details about the KEMP 360 Central version 1.8 features.

18.1 New Features

1. **Virtual Service Motion**

Provides customers the ability to migrate Virtual Services between LoadMaster devices that are being managed within KEMP 360 Central.

2. **Real Server Health Checks**

Enhancing the Virtual Service configuration to facilitate LoadMaster Real Server Health Check configuration.

3. **AWS ELB**

It is now possible to add/edit/remove AWS Elastic Load Balancing (ELB) and visualize key traffic metrics and statistics from the KEMP 360 Central User Interface (UI).

18.2 Feature Enhancements

1. Enhancing the licensing capabilities to allow KEMP 360 Central be licensed using a condensed format licensing string for closed network environments.

2. Providing the ability to allow KEMP 360 Central access to the internet using HTTP(S) proxy.

3. Provision of confirmation step on device reboot.

19 Version 1.7

Refer to the sections below for details about the KEMP 360 Central version 1.7 features.

19.1 New Features

1. **System Updates**

Providing the ability to perform an online (or offline) update of KEMP 360 Central firmware.

19.2 Feature Enhancements

1. Enhancing the licensing capabilities to allow KEMP 360 Central to be licensed offline.

20 Version 1.6

Refer to the sections below for details about the KEMP 360 Central version 1.6 features.

20.1 New Features

1. **Cert. based integration to LoadMaster**

Enhanced integration with LoadMaster devices to use certificates.

> Only available with LoadMaster v7.1.35 releases and above.

2. **SSH Access Control**

Allowing SSH access to KEMP 360 Central to assist with issue diagnosis and resolution

3. **MELA Licensing**

Providing alternative consumption models for KEMP customer base to facilitate flexibility in deploying large volumes of Virtual LoadMasters whilst maintaining control over their total cost.

20.2 Feature Enhancements

There are no feature enhancements as part of this release.

21 Version 1.5

Refer to the sections below for details about the KEMP 360 Central version 1.5 features.

21.1 New Features

1. **HAProxy**

It is now possible to add/edit/remove HAProxy devices and visualize key traffic metrics and statistics from the KEMP 360 Central UI.

2. **NGINX**

It is now possible to add/edit/remove HAProxy devices and visualize key traffic metrics and statistics from KEMP 360 Central UI.

3. **Public Cloud Certification**

KEMP 360 Central has been certified in both Azure and AWS.

21.2 Feature Enhancements

1. Checksums are now available (MD5/SHA) to ensure that all deliverables can be verified by customers.

22 Version 1.4

Refer to the sections below for details about the KEMP 360 Central version 1.4 features.

22.1 New Features

1. **Virtual Service management**

It is now possible to perform some Virtual Service management tasks, such as adding, removing and viewing basic properties.

2. **Virtual Service monitoring**

Virtual Service status is now displayed.

3. **Usage files**

KEMP 360 Central now gathers usage statistics which can be exported.

4. **Scheduling**

It is now possible to schedule activities, such as reboots, firmware updates and backups.

22.2 Feature Enhancements

1. It is now possible to configure the network options using the KEMP 360 Central console.

2. It is now possible to add, modify and delete SubVSs using KEMP 360 Central.

3. Enhancements have been made to the User Interface (UI).

4. Tooltip text has been added.

5. Security enhancements have been implemented.

6. Improvements have been made to the monitoring graphs.

7. Several styling enhancements have been made.

8. Navigation improvements have been made.

9. The Open WUI link is now hidden for the read_only user.

10. A date selector has been added to the metrics data download option.

11. A pop-up message now appears before updating the KEMP 360 Central software asking if you want to continue with the update.

12. A warning pop-up message now appears if a LoadMaster with a firmware version older than 7.1-30b is being added.

59

23 Upgrade Path to the Latest Release

The KEMP 360 Central firmware version is available on the **About** page, displayed by clicking on the question mark button on the bottom-left of the UI.

The following graphic summarizes the path that you need to follow to upgrade currently deployed KEMP 360 instances to the latest release.

Version	Upgrade Path
Pre-1.6	Upgrade to **V1.9** only. Contact KEMP Support to upgrade.
1.6	Upgrade to **V1.9** only. Contact KEMP Support to upgrade.
1.7 1.8	Upgrade to **V1.9** only (see the following section).
1.9	Upgrade to latest release is supported. Note that customers running a v1.9 image earlier than **v1.9.0.1403** must upgrade to **v1.9.0.1403** before upgrading to a later release.
1.12 to 1.24	Upgrade to latest release is supported.
1.25.2	Latest release.

23.1 Upgrading from Versions 1.7 and 1.8 to Version 1.9

This section tells you how to upgrade from KEMP 360 Central Versions 1.7 and v1.8 to Version 1.9. Customers running Version 1.6 and below should contact KEMP support for upgrade instructions.

1. Contact KEMP support for the location of the KEMP 360 Central **v1.9.0.1403** patch and download the patch to the local system from which you access the KEMP 360 user interface.

2. Open the KEMP 360 Central UI and click the gear icon (**Settings and Configuration**) in the bottom-left corner.

3. Click **Firmware Management**.

4. Click **Select Firmware**.

5. Browse to and select the KEMP 360 Central **v1.9.0.1403** patch from your local system.

6. Click **Upload & Install**.

7. A message appears asking if you want to proceed with the update. Click **Continue** to proceed.

8. After the update, KEMP 360 Central reboots.

Once the above is complete, you can use the UI to upgrade to the latest firmware release.

24 Appendix: Quick Start for Monitoring LoadMaster HA

In Version 1.19, a new device type (LoadMaster HA Pair) has been added to help you more effectively monitor the high availability (HA) services hosted on LoadMasters configured into HA pairs. This section will tell you what you need to know to get started using it.

> If you are upgrading to V1.19 (or a later release) from a release prior to V1.19, see the section **See the KEMP 360 Central Feature Description on our website for additional feature documentation.**

> for advice on how to modify your current configuration to use LoadMaster HA Pair devices.

24.1 Prerequisites

Before you create a LoadMaster HA Pair device ensure that:

1. The two LoadMaster HA mode units participating in the HA pair have already been added to Central as LoadMaster type devices.

2. The two LoadMasters are available (up) and communicating successfully with Central – their icons must be green or blue in the network tree.

3. You have available the IP addresses and ports of the two HA mode LoadMasters, as well as the shared IP address and port used by the HA configuration.

24.2 Creating a LoadMaster HA Pair

After you ensure the prerequisites in the previous section are complete, do the following to configure two HA mode LoadMasters into a LoadMaster HA Pair:

1. Click on the **Network and Device Administration** icon at left.

2. Click on the + icon at lower left to open the **Add a Device** screen.

3. Enter or select the parameters shown in the table below:

Parameter	Description
Device Type	Select L**oadMaster HA Pair**.
HA Shared IP : Port	Enter the **IP address** and **port** of the HA shared IP address used by the HA LoadMasters.

Nickname	(Optional) A name for the device that will appear in the network tree at left and elsewhere in the UI.
Username Password	The username and password for the HA configuration. This username and password combination must be defined on both LoadMasters.
HA1 IP : Port	Select the LoadMaster configured as HA1 in the LoadMaster WUI's HA Configuration page.
HA2 IP : Port	Select the LoadMaster configured as HA2 in the LoadMaster WUI's HA Configuration page.

4. Click **Apply**.

The Shared IP Address (or Nickname, if you supplied one) will now appear in the appropriate place in the network tree at left, with the two HA mode LoadMasters organized underneath, as shown in the example below.
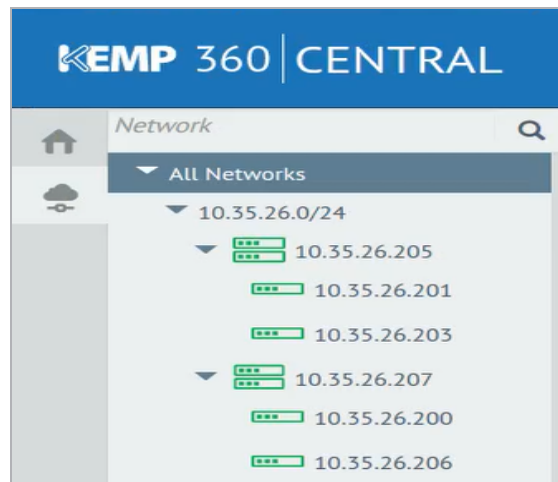
Please note the following:

- Most monitoring and service configuration is available by clicking on the Shared IP Address (or Nickname) device in the left frame. In the screen shot above, the shared IP device is 10.35.26.205.
- The Monitoring page for the shared IP device shows consolidated status across the HA pair.
- System configuration options specific to each of the LoadMasters are available by clicking on the icons underneath the shared device.
- See the section for a list of LoadMaster HA Pair issues and workarounds.

See the KEMP 360 Central Feature Description on our website for additional feature documentation.

24.3 Possible Adjustments After Upgrade from a Version Before 1.19

If you are upgrading from a release previous to V1.19 to V1.19 or a later release, you may need to adjust your current device list to take advantage of the new LoadMaster HA Pair device type introduced in V1.19. Specifically:

1. If you have added a device using the **HA Shared IP** for a pair of LoadMasters configured into an HA pair, then you must remove that device from Central before you can configure the **LoadMaster HA Pair** device. If you do not, then you'll get an error that the shared IP address already exists when trying to add the LoadMaster HA Pair device. The workaround is to remove the device using the HA Shared IP and try again.

2. If you have not already created two Central devices for the individual HA LoadMasters in the pair, then you must add them to Central before you can configure the **LoadMaster HA Pair** device.

Last Updated Date

This document was last updated on 01 October 2018.