KEMP 360 Central

Version 1.21

Release Notes

VERSION: 16.0

UPDATED: January 2018

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* on page 40.

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 & 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 Number of Managed Devices

A single instance of KEMP 360 Central can host a maximum of **150 managed devices**, with a **combined total of 2850 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.

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 handy. After you file a request, a KEMP Support Engineer will get in touch with you promptly.

2 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.

2.1 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.

2.2 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.

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, please contact KEMP support for more information on that issue.

ID	Description
KTS-4124	The Graphs page will display abbreviations for very large amounts of data in the Y-axis of various graphs, without providing a label for the abbreviations. For example: if the number of bytes returned in a network graph is above one quintillion (10^{18}), the numbers in the Y-axis will be followed by 'E', which stands for 'exabytes'.
KTS-3876	When 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 in 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 will close while the 'Add a Device' dialog 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 VSs and RSs for the HA nodes. The workaround is to use the Text search box instead.
KTS-3850	When Central is configured into HA mode with another instance of Central, restoring a backup archive taken from the Master onto the Standby unit will break the HA configuration.
KTS-3844	If a VS uses a wildcard (*) IP address, Real Servers cannot be added to the VS from Central. The workaround is to add them using the LoadMaster UI; they will then be displayed in the Central UI.
KTS-3837	**LoadMaster HA Pairs**: If the Shared IP Address for a LoadMaster HA Pair cannot be contacted, both HA units will show their status as 'Standby'. Access to the shared IP address from Central needs to be restored to correct the issue. Possible causes are that the Shared IP address's network is unreachable or that the authentication parameters on one or both of the HA units in the pair has been modified on LoadMaster without making the same modifications on Central.

ID	Description
KTS-3814	**LoadMaster HA Pairs**: If the two HA devices in a LoadMaster HA Pair take significantly different times to poll (e.g. HA1 takes 1 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 RBAC for a user on LoadMasters configured into HA mode, be sure to assign the same level of access to all 3 devices in the LM HA Pair -- the HA1 device, the HA2 device, and the Shared IP device.
KTS-3721	**LoadMaster HA Pairs**: If a LoadMaster HA unit configured into a LoadMaster HA Pair is moved to 'Standalone' mode in the LoadMaster WUI, the effect on status reporting for that device in the Central UI depends on the LMOS release: • If the now standalone mode device is running LMOS release **7.2.37 or later**, that unit's device in Central will always show as 'down' in the Central UI. • If the now standalone mode device is running an LMOS release **earlier than 7.2.37**, the unit will always show its HA status as 'Standby', even when it is 'Active'. The only indication you will get that there is some problem is that the now standalone unit will never assume the 'Active' role, even when the other unit is unavailable.
KTS-3705	If a LoadMaster that is licensed for Metered Licensing Agreements (MELA) is upgraded during the course of a month, two MELA reports will be sent
KTS-3438	In the log viewer, it is possible for the user to mis-configure a **Time Range** (e.g., set a **From Date** *later* than a **To Date**), and then select another range (e.g., **Last Week**). If the user then tries to export the log display, the export will fail because the invalid **From** and **To** dates are still being checked, even though they do not apply to the **Last Week** selection.
KTS-3432	Once set to a non-null value, the nickname and alternate address of a VS cannot be cleared (reset to no value) from KEMP 360 Central; the workaround is to clear these parameters using the LoadMaster WUI.
KTS-3427	Errors can occur when selecting multiple devices in the 'System Reboot', 'Templates', 'Update LoadMaster Firmware', and 'Backup/Restore' accordions on the 'System Configuration' tab at the network level. If such errors are seen, the workaround is to use the 'System Configuration' tab at the device level instead.
KTS-3390	When AWS ELB devices are present in the configuration, it is possible for status information for all devices to be delayed, such that status information is processed and visible in the UI on a 2-minute cycle, instead of every minute.

ID	Description
KTS-3373	If you attempt an operation that requires SMTP parameters to be set, but they are *not* set, then multiple error messages will be displayed by the UI. The first of these messages contain the actual error (e.g., email address not set), while the rest contain no pertinent information.
KTS-3304	If a user login is created, given full write permission, and added as a member of a custom user group – then any device added by that user will not be seen by that user in the network tree. The workaround is to specifically add the new device to the custom group.
KTS-2862	When selecting a backup file for restore on a managed device, the UI only displays the last 20 archives created.
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 VS should both enable Layer 7 services on the VS 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 VS motion, the virtual IP address and port to use for the new VS is not automatically updated when you select a LoadMaster from the 'Target' drop-down box. 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.

2.3.1 Known Issues with Specific LoadMaster Releases

The table below lists issues seen on 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	**ASL 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 will be addressed in LMOS Version 7.2.41.
PD-9947	Issues with VS status returns from LoadMasters running version 7.1.35.4 can result in incorrect VS health status being displayed in the Central UI. This can occur when either VS status is requested from the LoadMaster or when the VS is modified (if the issue is not already present). In the latter case, the issue should correct itself on the next UI status update (i.e., within a minute).

ID	Description
PD-9747	When monitoring two LoadMasters that are configured into an HA pair, and certificate authentication is being used, 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 will have no effect on traffic through the HA pair (since 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'. 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. However, because of an issue in the LoadMaster API, quotes and spaces in LoadMaster passwords can cause authentication from KEMP 360 Central to fail -- while they work without issue when logging directly into the LoadMaster WUI. Until this issue is addressed in the LoadMaster API, you should log in to 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.

1 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.

1.1 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.

2 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.

2.1 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.

2.2 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.

3 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.

3.1 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.

3.2 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.
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).

ID	Description
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).

4 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.

4.1 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.]

4.2 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).

ID	Description
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 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.

ID	Description
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 insecurely.

5 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.

5.1 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.

5.2 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.

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.

6 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.

6.1 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.

6.2 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*, above.

6.3 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 **Non-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.

6.4 Issues Resolved

ID	Description
Various	Improved UI performance through a number of internal changes. See *System Sizing Limitations* on page 25 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 Management to consistently use the Year-Month-Day format.

ID	Description
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.

7 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.

7.1 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*.

7.2 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.

ID	Description
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.

8 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.

8.1 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.

8.2 Feature Enhancement

1. Virtual Service heat maps have been removed.

8.3 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.

ID	Description
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.

9 Version 1.8

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

9.1 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).

9.2 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.

10 Version 1.7

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

10.1 New Features

1. System Updates

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

10.2 Feature Enhancements

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

11 Version 1.6

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

11.1 New Features

1. Cert. based integration to LoadMaster

   Enhanced integration with LoadMaster devices to use certificates.

   Note: 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.

11.2 Feature Enhancements

There are no feature enhancements as part of this release.

12 Version 1.5

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

12.1 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.

12.2 Feature Enhancements

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

13 Version 1.4

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

13.1 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.

13.2 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.

14 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 **1.20**	Upgrade to latest release is supported.
1.21	Latest release.

14.1 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.

15 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.

Possible Adjustments After Upgrade from a Version Before 1.19 for advice on how to modify your current configuration to use **LoadMaster HA Pair** devices.

15.1 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.

15.2 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:

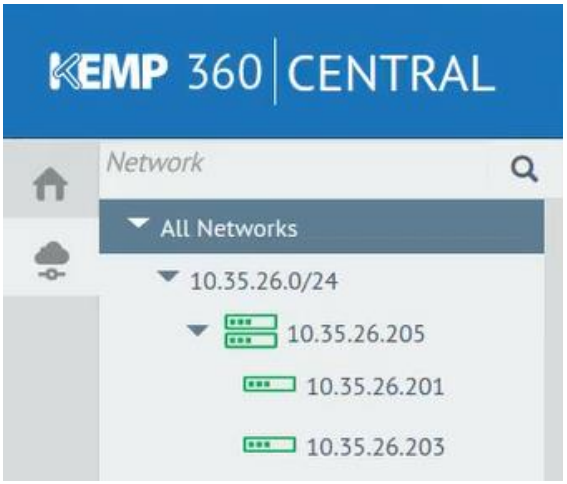
1. Click on the **Network and Device Administration** icon at left.
2. Click on the + icon at lower left to open the **Add a Device** screen.
3. Enter or select the parameters shown in the table below:

Parameter	Description
Device Type	Select **LoadMaster 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.

Parameter	Description
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.

15.3 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.

Document History

Date	Change	Reason for Change	Ver.	Resp
Jan 2016	Initial document	Version 1.1 release	1.0	LB
Jan 2016	Minor change	Updated Copyright Notice	2.0	LB
Feb 2016	Release updates	Version 1.2 release	3.0	LB
Apr 2016	Release updates	Version 1.4 release	4.0	LB
Aug 2016	Release updates	Version 1.8 release	5.0	LB
Sep 2016	Release updates	Version 1.9 release	6.0	LB
Jan 2017	Release Updates	Version 1.12 release	8.0	MRH
Mar 2017	Release Updates	Version 1.14 release	9.0	MRH
Apr 2017	Updated Section 1.2	Added MELA-specific guidelines	9.1	MRH
May 2017	Release Updates	Version 1.15 release	10.0	MRH
Aug 2017	Release Updates	Version 1.17 release	12.0	MRH
Sep 2017	Release Updates	Version 1.18 release	13.0	MRH
Nov 2017	Release Updates	Version 1.19 release	14.0	MRH
Dec 2017	Release Updates	Version 1.20 release	15.0	MRH
Jan 2018	Release Updates	Version 1.21 release	16.0	MRH