Kemp 360 Central

Feature Description

UPDATED: 21 August 2020

Copyright Notices

Table of Contents

1 Introduction

Kemp 360 Central is a centralized management, orchestration, and monitoring application that simplifies and accelerates the configuration and management of LoadMaster load balancing resources.

Kemp 360 Central provides critical features for managing application delivery and acceleration in modern heterogeneous IT infrastructures. With it, users can easily:

- Deploy new LoadMaster instances using the User Interface (UI) or Application Programming Interface (API)
- Manage the application lifecycle with configuration management using the UI or API
- Monitor performance and usage statistics of the networks, sub-networks, and LoadMasters (including any Virtual Services, Real Servers and SubVSs), which are attached
- Monitor third party products such as Amazon Web Services (AWS) ELB, HAProxy, NGINX and F5 BIG-IP.
- Monitor Virtual Services at both network and LoadMaster level
- Monitor Real Servers at both a network and LoadMaster level
- Schedule device maintenance including firmware updates, reboots, and backups
- Deploy Kemp 'best practice' templates to LoadMaster devices
- Back up and restore LoadMasters centrally
- LoadMaster log collection and analysis

Kemp 360 Central should only be used to manage LoadMasters that have firmware version 7.1-30b or above installed.

LoadMasters with firmware between 7.1-26 and 7.1-30b have reduced statistics functionality.

Kemp 360 Central does not work with LoadMaster firmware below 7.1-26.

Kemp 360 Central is only available on certain subscriptions. Please contact a Kemp representative if needed.

1.1 Document Purpose

This document provides details on each of the functions that are available in Kemp 360 Central.

1.2 Intended Audience

This document provides guidance for configuring and managing a multi-vendor, multi-platform ADC fabric using Kemp 360 Central.

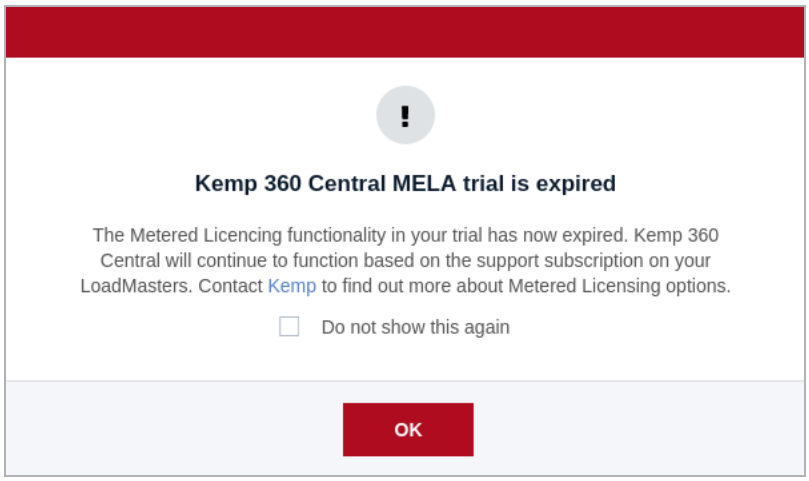
2 Activation and Initial Login

Kemp 360 Central offers a number of licensing options depending on whether you are taking a trial, using Metered or Pooled licensing, or licensing through a LoadMaster support subscription. A Contract/Order ID is not required when licensing a trial.

> A Contract/Order ID is necessary for Metered licenses while an Order ID is used for standard licenses.

Kemp 360 Central Trial Licensing

Licensing a trial does not require an Order or Contract ID. During the trial period, you can license and manage up to five Metered-licensed LoadMasters and monitor up to 25 pre-licensed LoadMasters. You can switch to a regular license at any stage during the trial period by re-licensing Kemp 360 Central with a valid Order or Contract ID.



When the trial period expires, all currently activated Metered Licensing licenses will die after a grace period and no more Metered Licensing licenses will be available.

> Once you convert a trial license to a permanent license, you cannot have a trial license again.

Licensing with an Order or Contract ID

If you have a Contract or Order ID, you can either select any of the licenses associated with that Contract/Order ID or you can select a trial license. To activate the license, select the license and click **Apply License**.

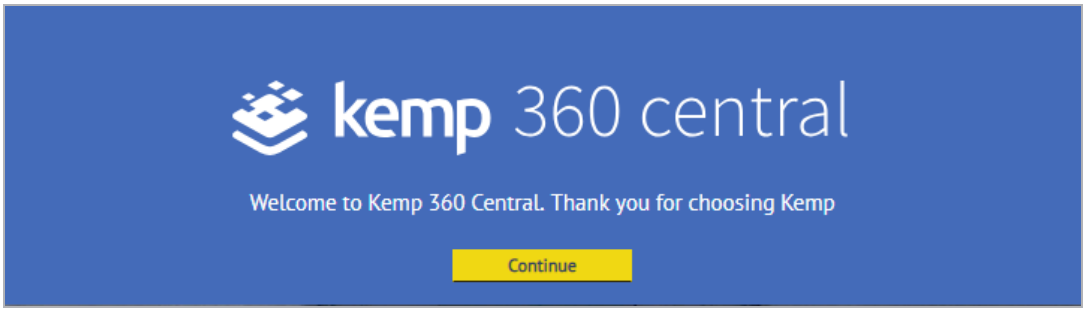
Activation

There are three methods to activate a license – online, offline, or manually. Use online if you have access to the internet. If you can access Kemp 360 Central but Kemp 360 Central cannot access the internet, a license can be obtained using the offline method. Manual licensing involves a verbal transfer and manual entry of a license. This is usually used when there is a network configuration or there are security requirements that prevent internet connectivity of network devices or administrative systems.

Online Licensing

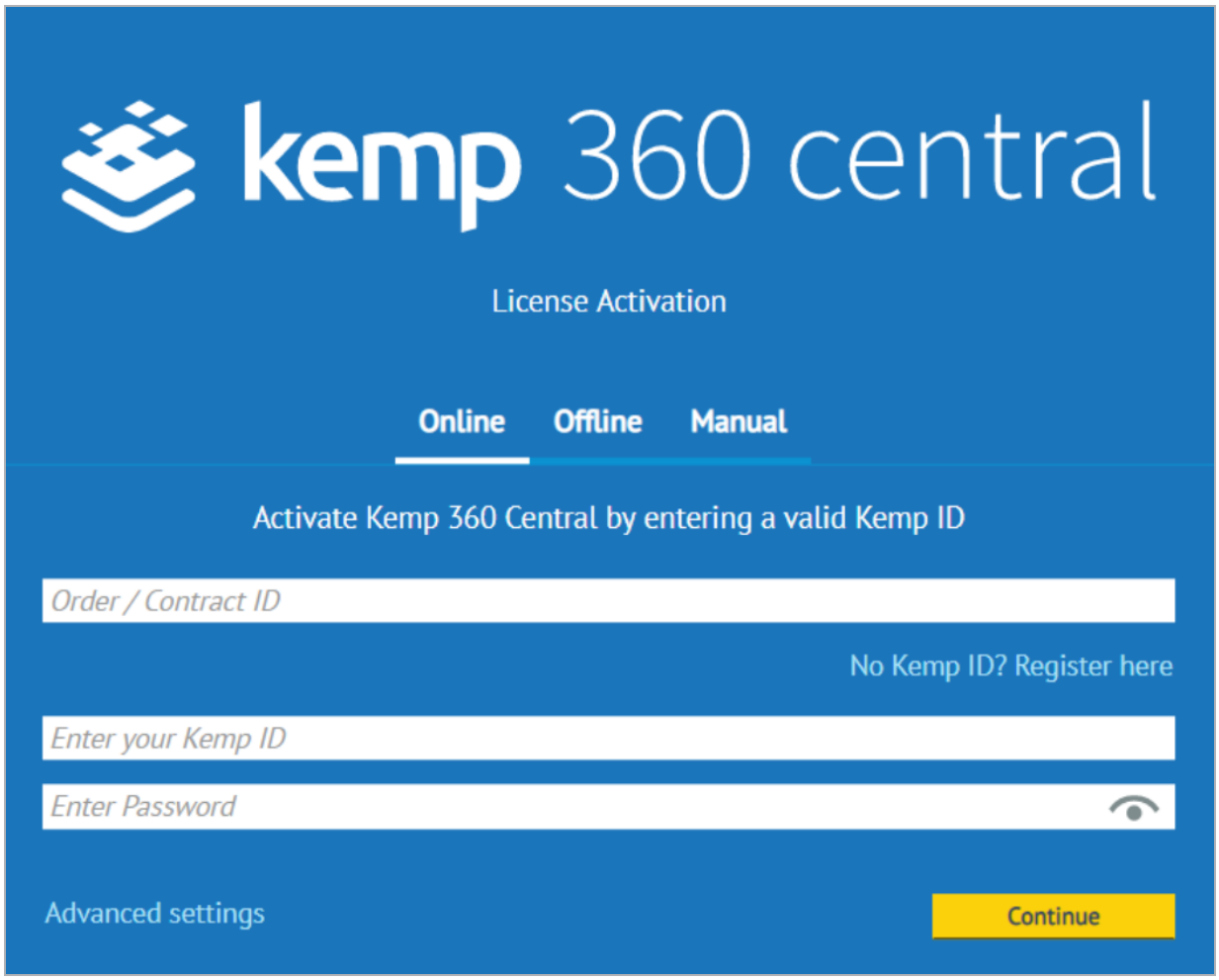
Perform the following steps:

1. To access the Kemp 360 Central user interface (UI), in your browser, enter the IP address of the instance. A license activation screen appears.



2. Click **Continue**.

3. The End User License Agreement (EULA) is displayed. Click **Agree** to accept the EULA and continue.

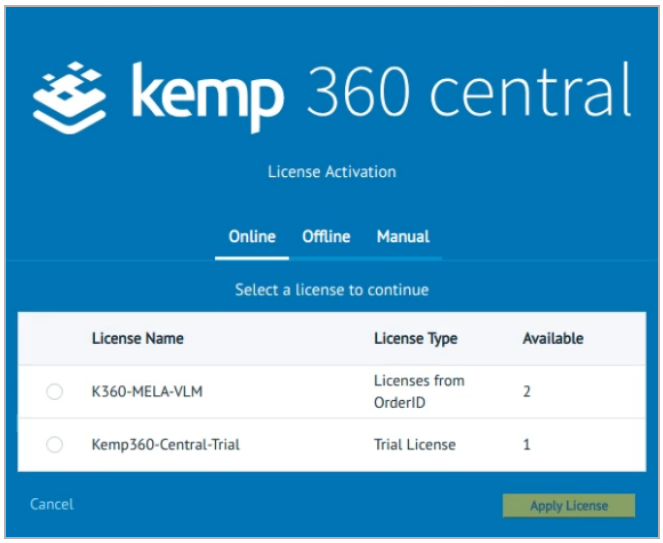


4. Enter your **Order** or **Contract ID** in the field provided.

5. Enter your Kemp ID (the email address used when registering the Kemp account). Users need a Kemp ID to license Kemp 360 Central. If you do not have a Kemp ID, click the link provided and register one.

6. Type your password. If you want to display the password while entering it, click the eye icon.

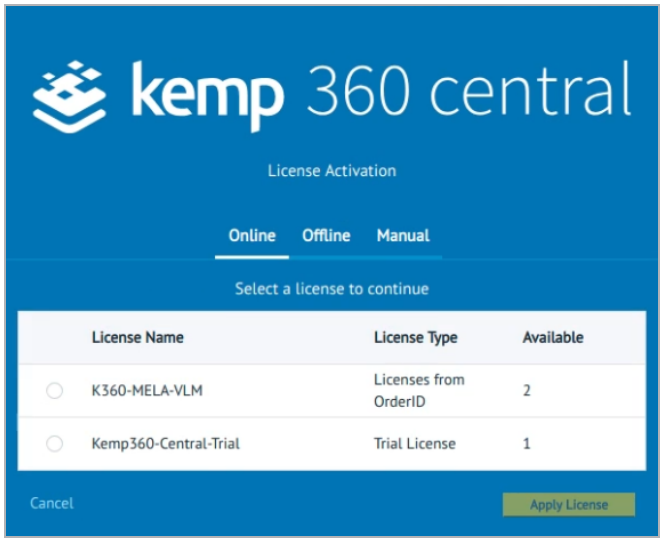
7. Click **Continue**.



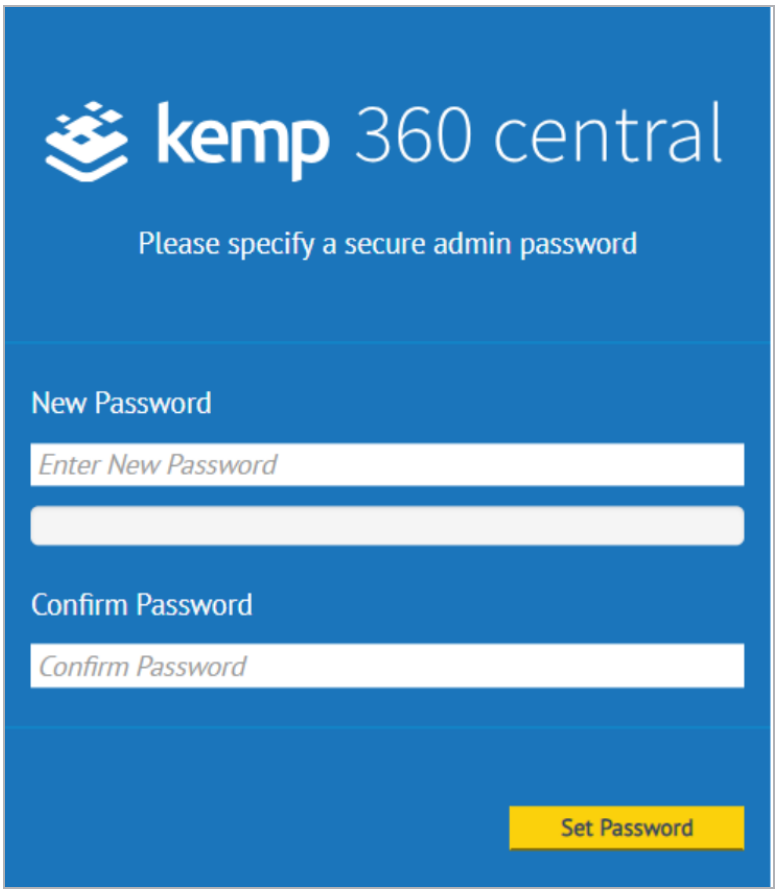
If you have no Order or Contract ID, the only option you can have is a trial license.

If you want to cancel or want to return to the previous screen, click **Cancel**.

8. To activate the license, select the license and click **Apply License**.



If you have an Order or Contract ID, you can either select any of the licenses associated with that ID or a trial license. To activate the license, select the license and click **Apply License**.

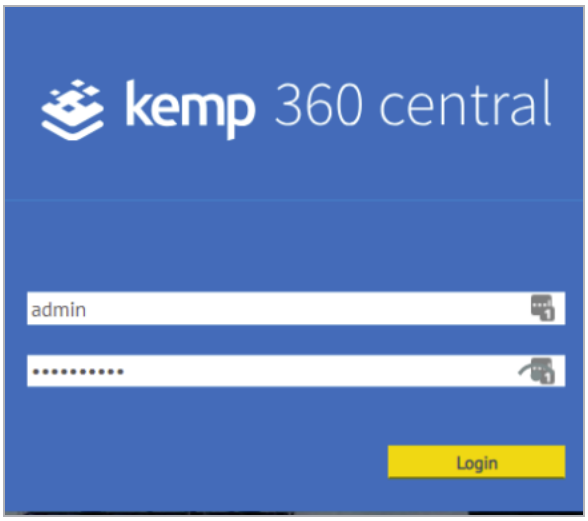


9. Enter a new admin password in the two text boxes provided and click **Set Password**.

> By changing the password here, you also change the password for the console.

> Passwords must be a minimum of eight characters long, contain at least one upper case letter and one number. All special characters are valid. See the **Appendix: Password Information** for more information.

The option to change or reset a user password by clicking the **Reset password** link should be used only if the current password is known.



> You may now log in to Kemp 360 Central as the **admin** user, using the password you created previously.

> The **admin** user has access to the full range of options in Kemp 360 Central and can define additional user logins.

The initial configuration of Kemp 360 Central is now complete.

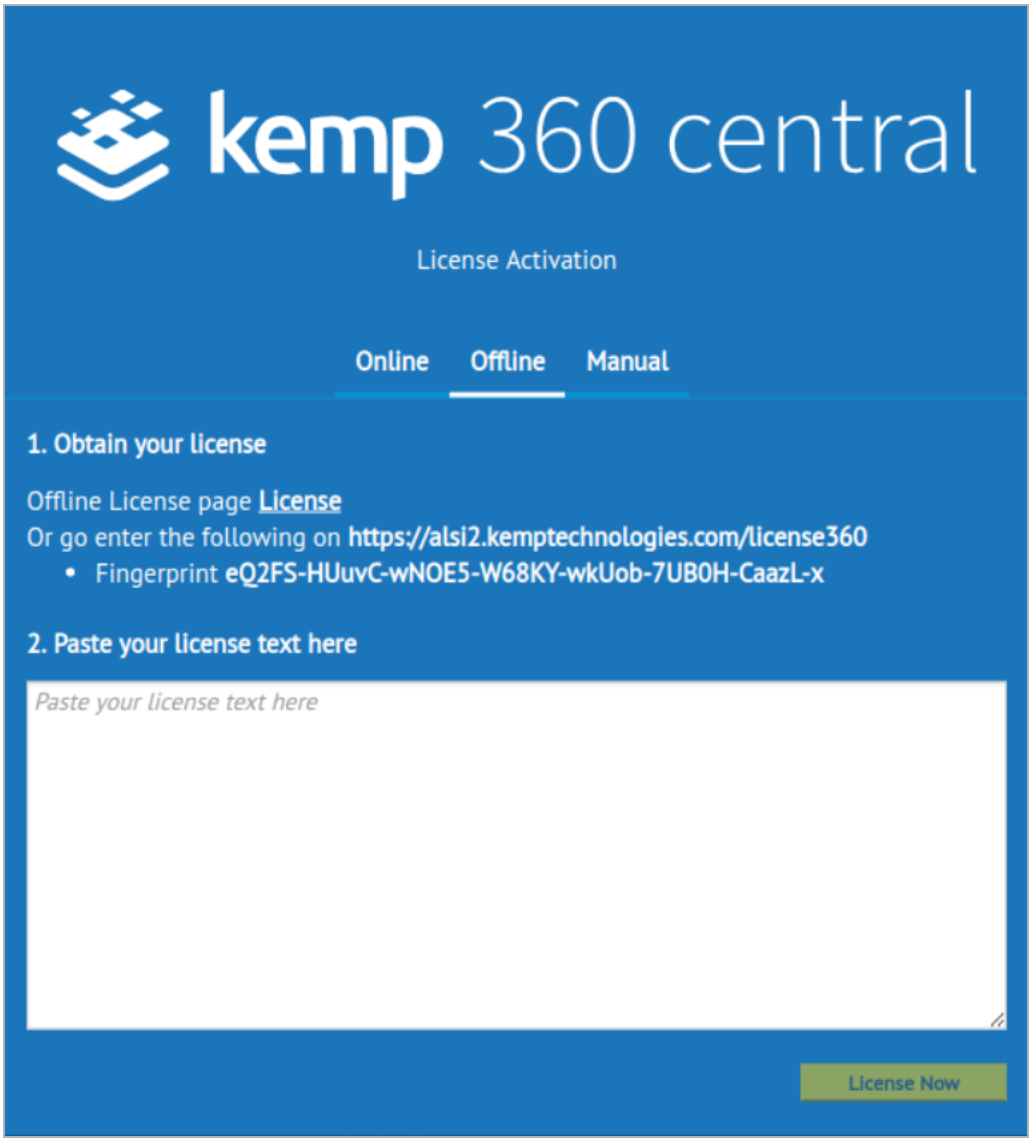
Offline Licensing

1. Access the Kemp 360 Central UI by entering the address in a web browser.

> Ensure you add **https://** before the address.

2. A warning may appear regarding website security certificates; click the **Continue**/**Ignore** option.

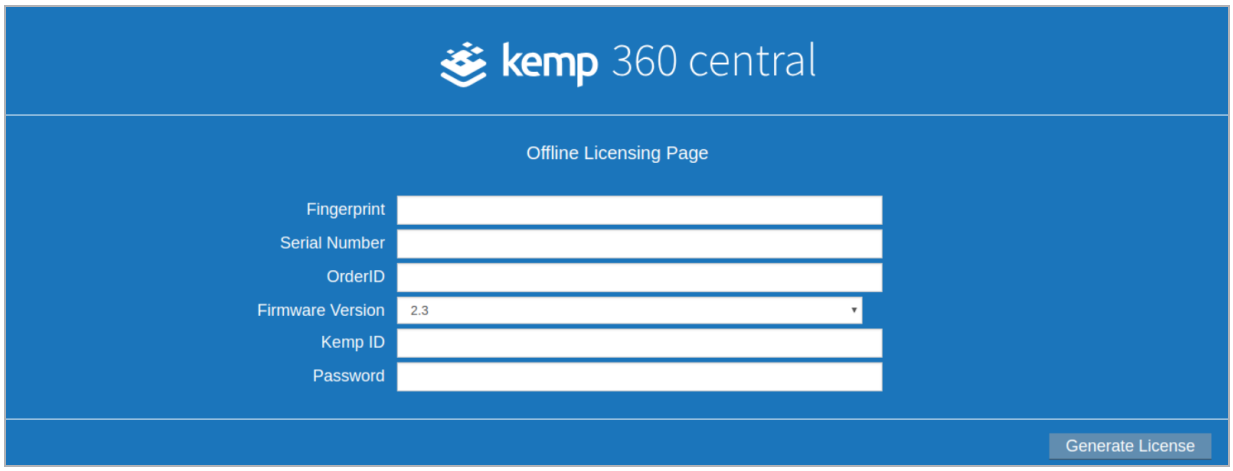
> If this is the first time accessing the UI, the End User License Agreement (EULA) may need to be accepted.



3. Select **Offline**.

4. Click the **License** link or go to the link provided on a computer that has internet access.

5. The **Fingerprint** and **Serial Number** are on the **Kemp 360 central** screen, if available. Copy them and enter them on the **Offline Licensing Page**, if available.



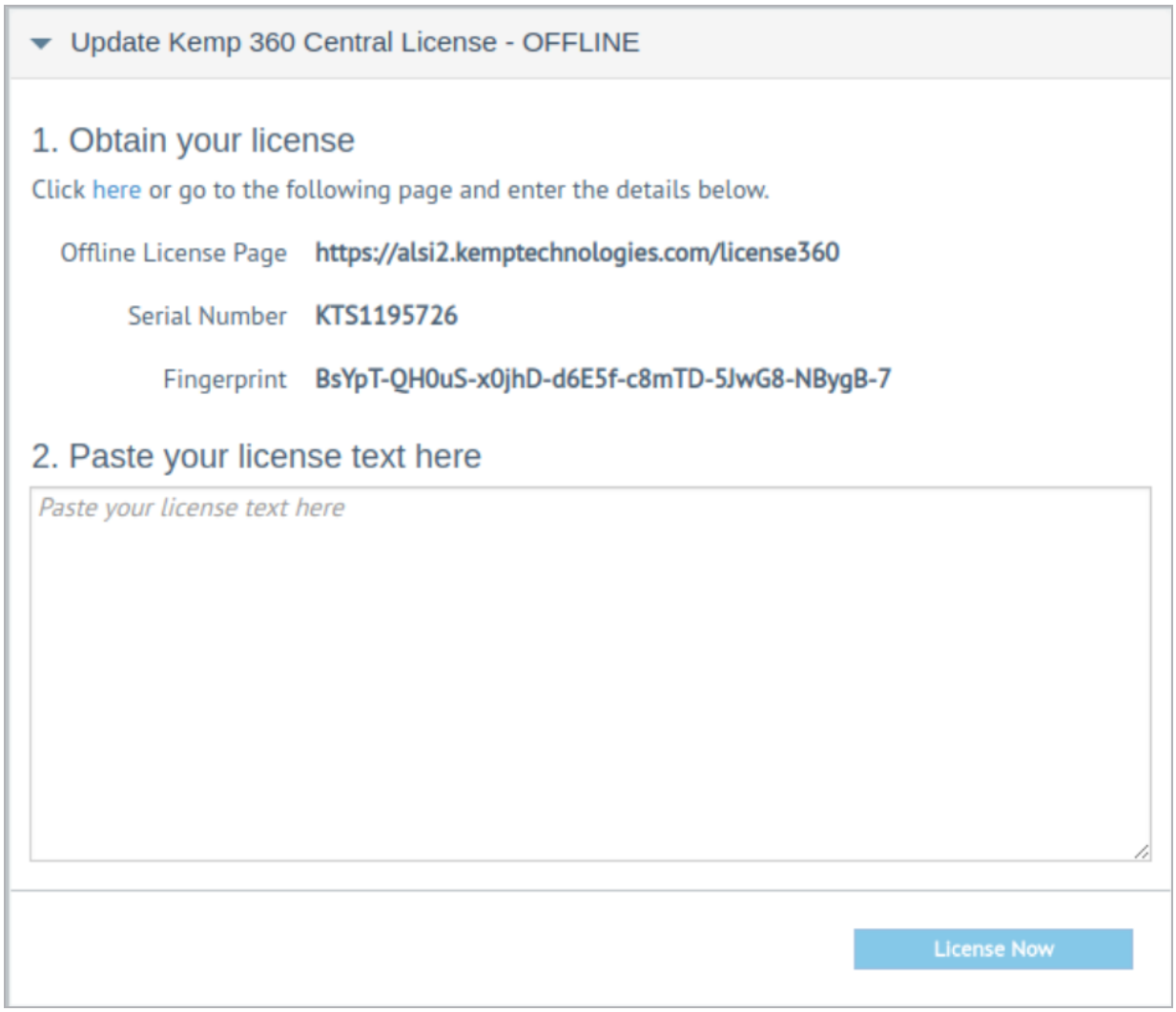
6. Enter an **Order ID** if you have one. The Order ID is provided by Kemp when a license is purchased.

7. Select the **Firmware Version**.

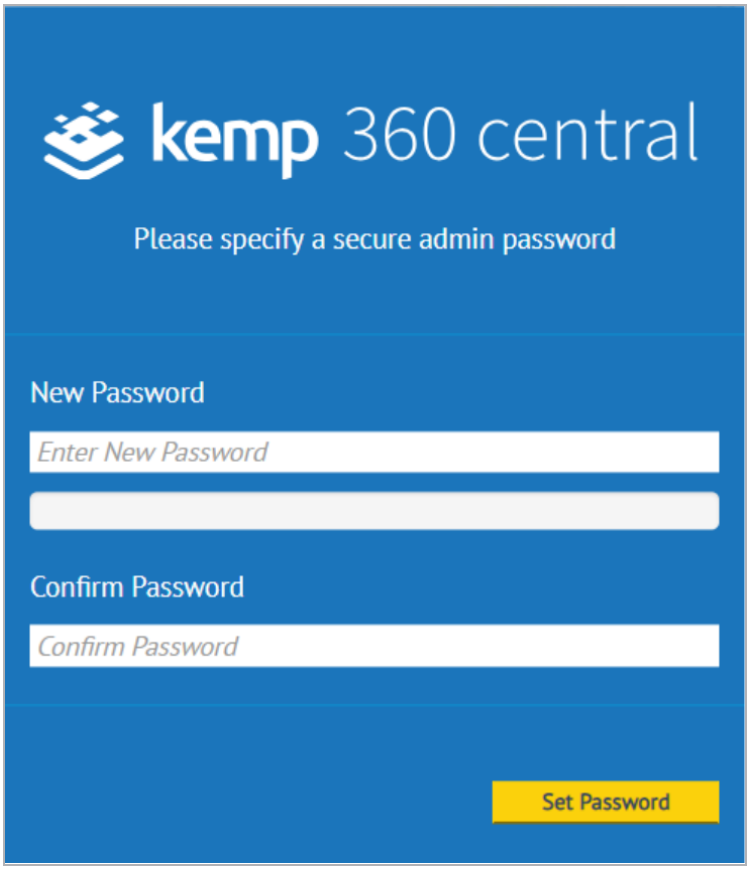
8. Enter your **Kemp ID** and **Password**.

9. Click **Generate License**. An email is sent to the Kemp ID specified. This email contains a section called **License Block**.

10. Copy the **License Block**.



11. In Kemp 360 Central - paste the **License Block** text into the text box provided.
12. Click **License Now**.



13. Enter a new admin password in the two text boxes provided and click **Set Password**.

> By changing the password here, you also change the password for the console.

> The bar in the middle represents the strength of the password. The fuller the bar is - the more secure the password is.

The initial configuration of Kemp 360 Central is now complete. If you receive any error during the process, contact Kemp Support.

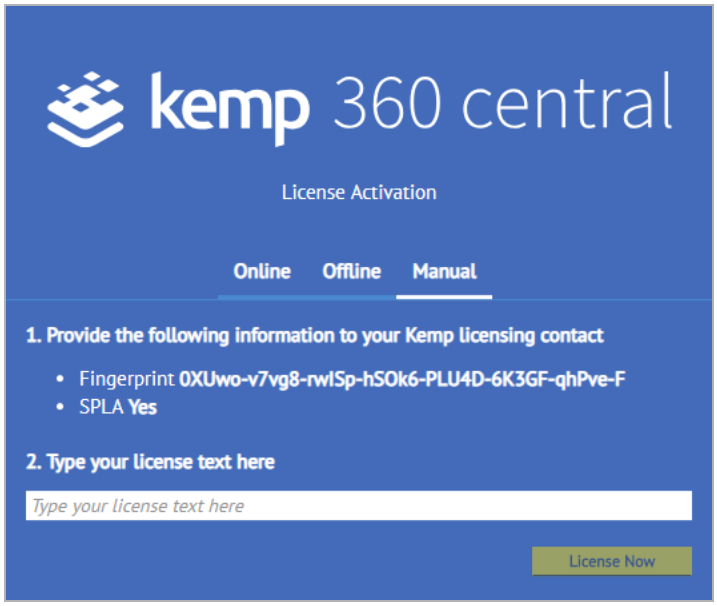
Manual Licensing

To license Kemp 360 Central using the manual method, follow the steps below:

1. Access the Kemp 360 Central UI by entering the address in a web browser.
2. Ensure to add **https://** before the address.

3. A warning may appear regarding website security certificates. Click the continue/ignore option.

> If this is the first time accessing the UI, the End User License Agreement (EULA) may need to be accepted.



4. Contact your Kemp licensing representative.

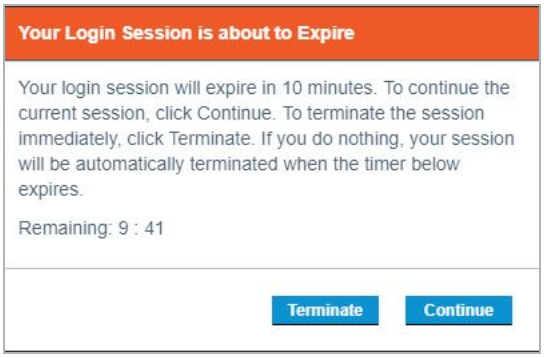
5. Provide the Kemp representative with the **Fingerprint**, which is displayed.

6. The Kemp representative will provide you with a 32-character license string that must be entered in the text box provided. Dashes are automatically added while typing.

7. Click **License Now**.

8. Return to step 8 of Online Licensing and complete the procedure.

Session Inactivity



If you are inactive on a Kemp 360 Central system for 24 hours, your UI session ends and you have to log in again. A dialog box appears 10 minutes before this time to notify you. The first time you log in, use the admin account with the password you specified in the previous step. You can then create additional user login accounts.

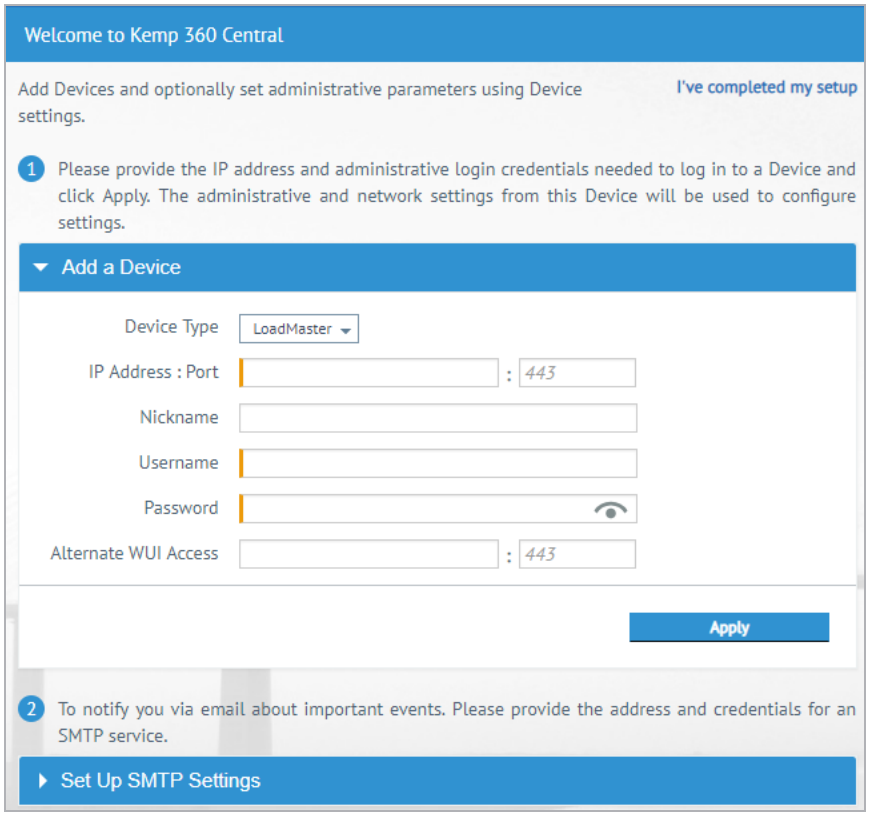
2.1 Logging Out

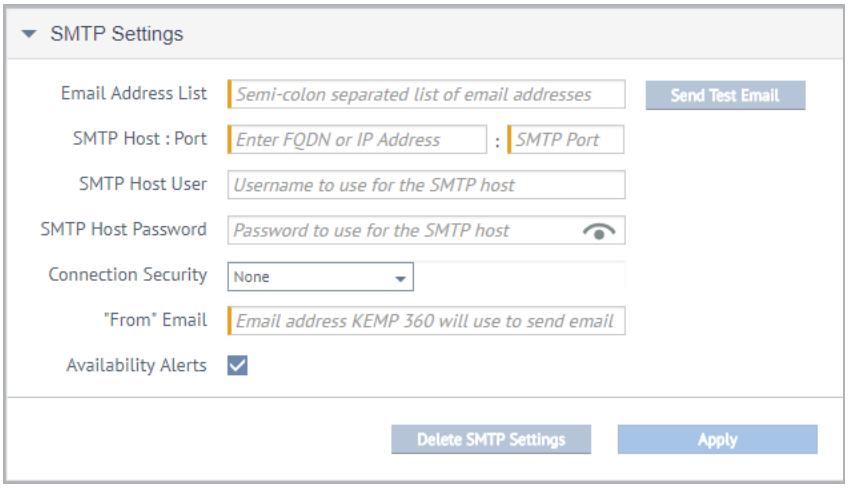
To log out of Kemp 360 Central, click the **logout** button, which appears in the top right of all screens.

2.2 Welcome Screen

When you configure your Kemp 360 Central for the first time, the **Welcome to Kemp 360 Central** screen opens. This screen enables you to add single LoadMasters, LoadMaster HA pairs, and third-party devices, and makes the process of configuring your Kemp 360 Central as quick and easy as possible. The **Welcome to Kemp 360 Central** screen also enables you to pre-populate the SMTP configuration with an existing configuration. This is covered in detail in the **Adding Devices** section.

Both steps are optional and can be skipped.





You may optionally add an ADC device and configure SMTP at this stage. The SMTP settings are populated from the newly added LoadMaster if there are currently no SMTP settings on Kemp 360 Central. Note that only the **Email Address List**, **SMTP Host**, **Port**, and **SMTP Host User** fields are pre-populated. You must type in the **SMTP Host User** and **SMTP Host Password** fields (if required by the SMTP server), as well as the **'From' Email** field. The **Availability Alerts** check box is enabled

by default. When this option is enabled, email notifications are sent when the status of a device changes.

You can access the **Welcome** screen anytime after your first login by clicking the **About and Help** (question mark) icon in the bottom left of the screen and then clicking **Welcome on Board**.

> The SMTP Setting pane is pre-populated from the LoadMaster if there are currently no SMTP settings on Kemp 360 Central. Note that only the **Email Address List**, **SMTP Host**, **Port** and **SMTP Host User** fields are pre-populated. You must type in the **SMTP Host User** and **SMTP Host Password** fields (if required by the SMTP server), as well as the **'From' Email** field. The **Availability Alerts** check box is enabled by default. When this option is enabled, email notifications are sent when the status of a device changes.

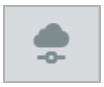
The above section describes how to configure these details in the **Welcome** screen. These details can also be configured elsewhere:

- Configure the administrator email settings (see the **SMTP Settings** section)
- Add a device (see the **Device Management** section)

3 Kemp 360 Central Interface Description

This section of the document describes the Kemp 360 Central interface.

- The **Global Dashboard** provides you with a high-level summary of the health and status of your devices. For more information, see the **Global Dashboard** section.



- The **Network and Device Administration** screen explains how networks and devices are managed in Kemp 360 Central. For more information, see the **Network and Device Management** section.

- The **Configuration Management** screen enables you to deploy LoadMasters and set up target environments. For more information, see the **LoadMaster Deployment** section.

- The **Global Repository** is used to upload files (such as firmware, template and backup files) to Kemp 360 Central. For more information, see the **Global Repository** section.

- The **Access Control** screen enables you to manage the different levels of access required by different users. For more information, see the **Access Control** section.

- The **Settings and Configuration** icon provides access to a number of options in Kemp 360 Central including license management, reporting, and logging.

- The **About and Help** sections are covered within this section.

- The **Product Feedback** icon takes you to a web page where you can provide direct feedback to Kemp.

3.1 About Screen

Clicking the question mark button on the bottom-left of the UI brings users to the Kemp 360 Central **About and Help** page. This page contains information about:

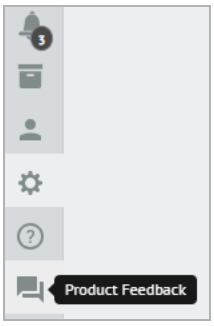
- The Kemp 360 Central license features (including a link to update the license)
- The Kemp 360 Central firmware version
- The boot time and uptime of Kemp 360 Central
- The Kemp 360 Central serial number, which is needed when contacting Kemp about support or license queries
- To view a list of open source licenses, click **View Licenses**. Click **View** to view the applicable license.

3.2 Help Screen

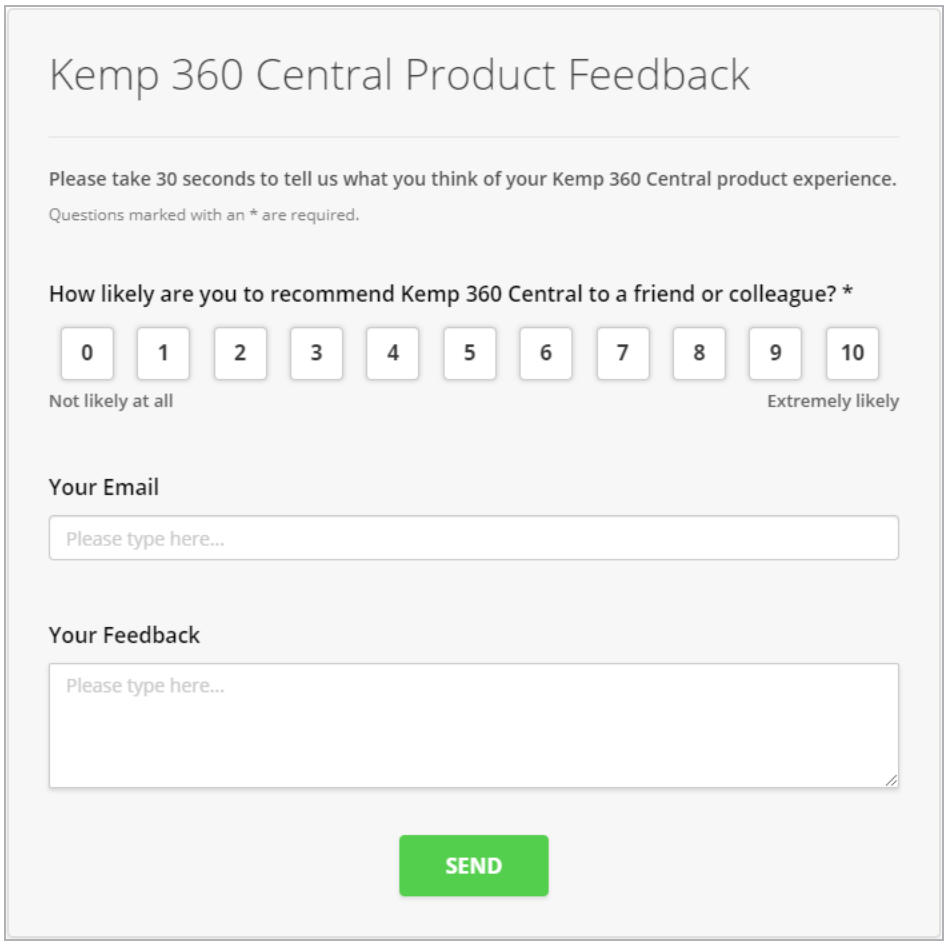
The **Help** screen provides a link to the Kemp Documentation page and the Kemp Customer Support site.

3.3 Product Feedback

You can provide direct feedback to Kemp using the **Product Feedback** feature.



To provide feedback, click the **Product Feedback** icon.

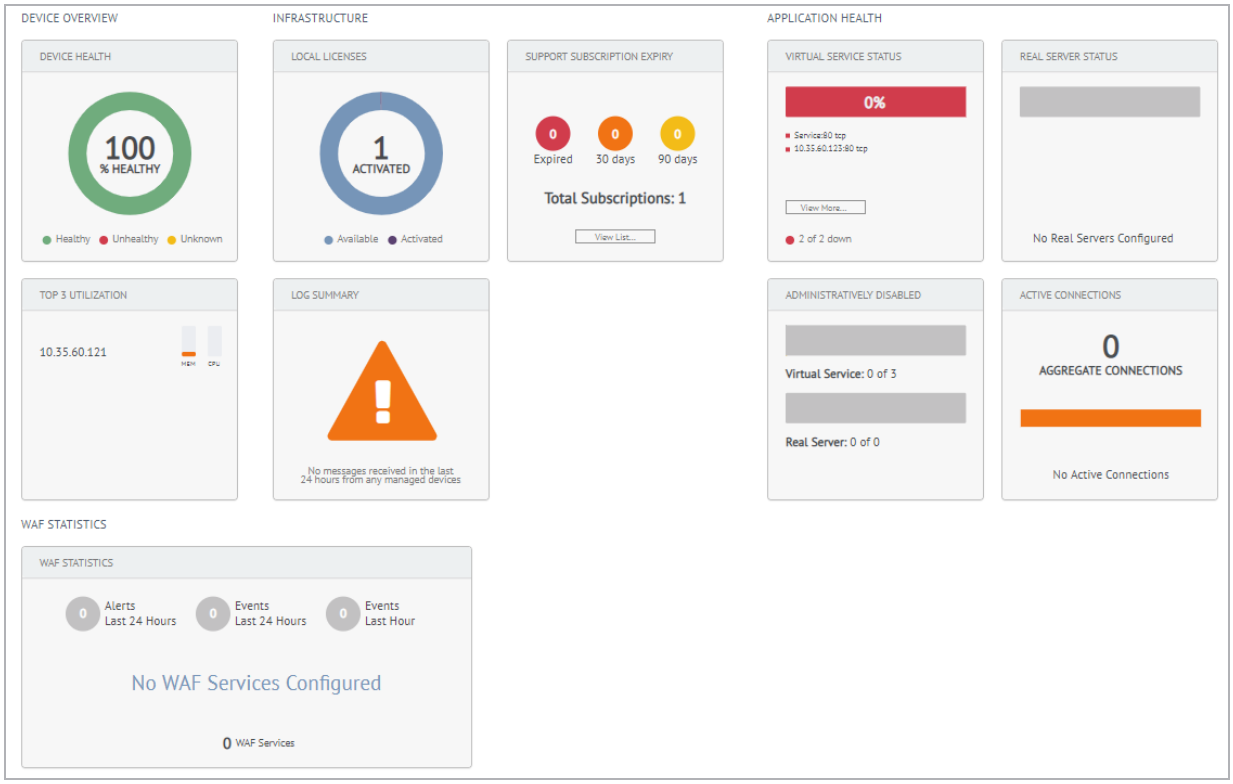


This opens a web page where you can decide how likely, on a scale of 0 to 10, you are to recommend Kemp to a friend or colleague. You can also provide specific feedback in the box provided.

4 Global Dashboard

References to ASL in screenshots should be read as Local Licensing.

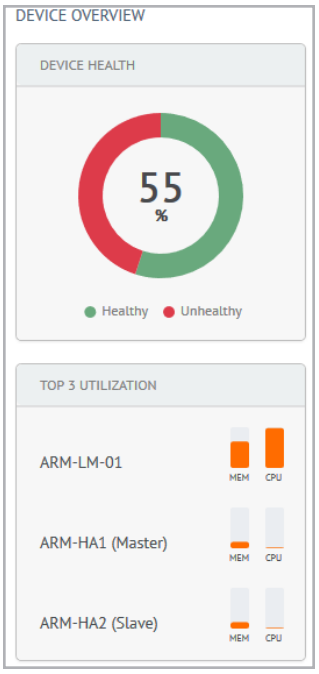
The Global Dashboard provides you with a high-level summary of the health and status of your devices. It contains the following sections that provide you with more detailed information relating to the status of your LoadMaster: **Device Overview**, **Infrastructure**, and **Application Health**. If you have WAF configured, there will be a section on WAF statistics.



4.1 Device Overview

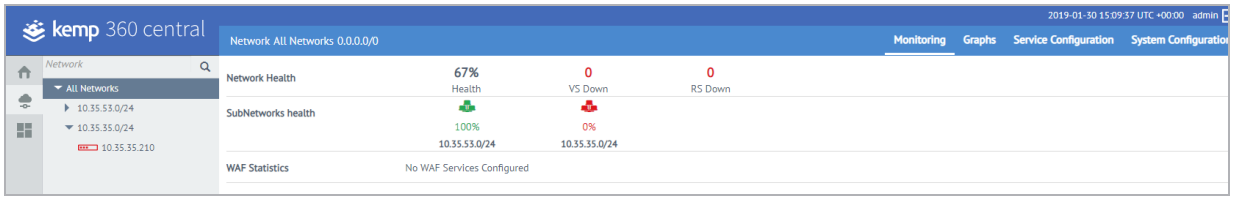
This section contains two panels: **Device Health** and **Top 3 Utilization**.

In the **Device Health** panel, you can quickly see what percentage of your devices are healthy and unhealthy. In the graphic below, the percentage of healthy devices is 55%.



The shared IP of a LoadMaster HA pair does not appear on this widget.

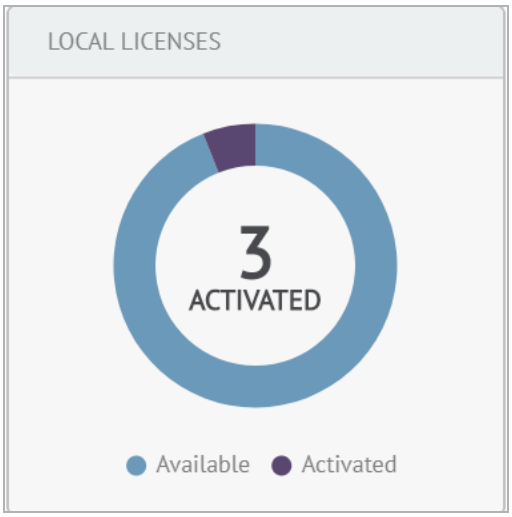
If you hover your mouse over the **Device Health** panel, it displays the number of healthy devices, unhealthy devices and unknowns (unknowns refer to devices that have never been successfully contacted by Kemp 360 and so their status is unknown). If you click the **Device Health** panel, you can view the health of your devices in more detail (see graphic below).



The **Top 3 Utilization** panel displays the top three resource consuming devices based on memory and CPU only. You can click each LoadMaster on this panel to view the Monitoring page for that device. However, if there are no devices configured, the **Welcome to Kemp 360 Central** screen appears.

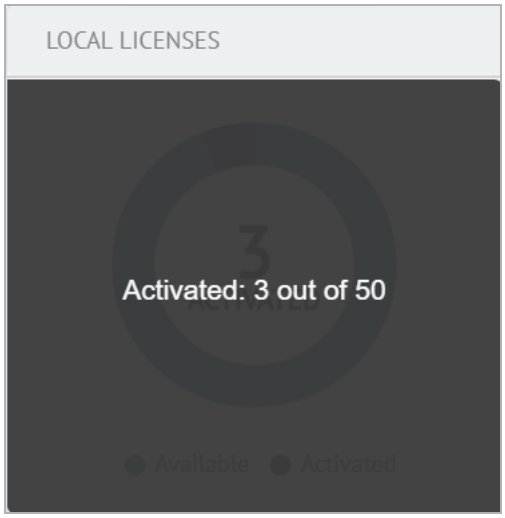
4.2 Infrastructure

The Infrastructure section contains two or three panels depending on your local configuration: **Local Licenses**, **Log Summary**, and **Support Subscription Expiry**.

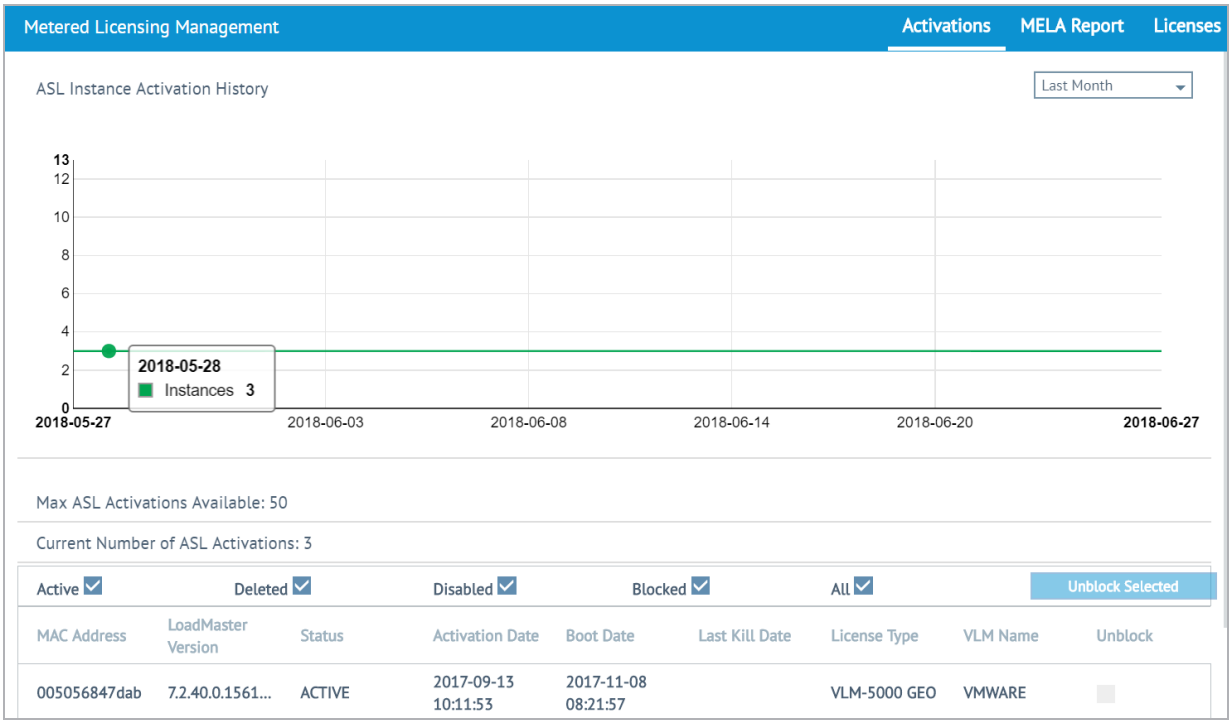


Local Licenses

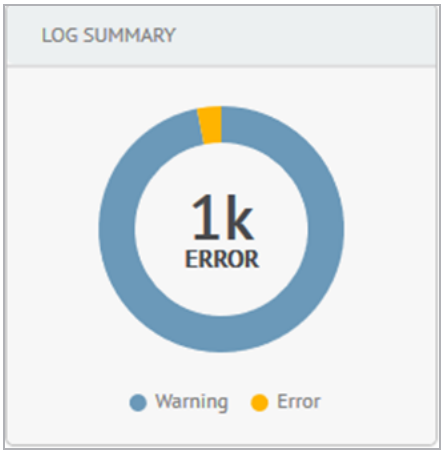
Local Licenses are licenses issued by Kemp 360 Central.



If you hover over the **Local Licenses** panel, you can see how many licenses are activated.



If you click the **Local Licenses** panel, the **LoadMaster Licensing** screen opens. Here you can view information on instances and report data.



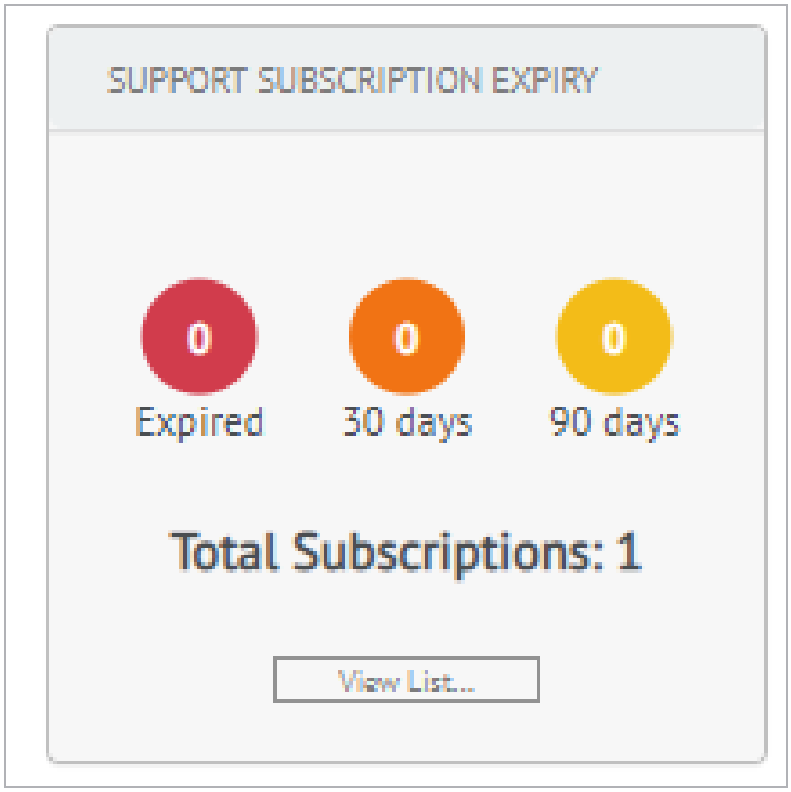
Log Summary

The **Log Summary** panel displays a circular color-coded chart where you can immediately tell the proportion of different types of errors including critical, errors, and warnings. This updates every second. If no messages are received for 24 hours, an orange exclamation mark will be visible. If you

click this panel, the **Logging** screen opens where you can filter the logs using several different criteria. See **Logging** for more information.

> The HA Shared IP Address of a LoadMaster HA pair is not a licensed device, and so is not represented in the dashboard licensing widgets. HA Shared IP Addresses also do not contribute logs to the Log Summary widget because no log messages come directly from the Shared IP, but instead from the IP addresses of the two HA LoadMasters.

Support Subscription Expiry



In the **Support Subscription Expiry** panel you can quickly identify the total number of local and non-local subscriptions. You can also quickly see the number of LoadMasters that are approaching or have passed their Support expiration date. These are color-coded as follows:

- Red: Expired
- Amber: 30 Days

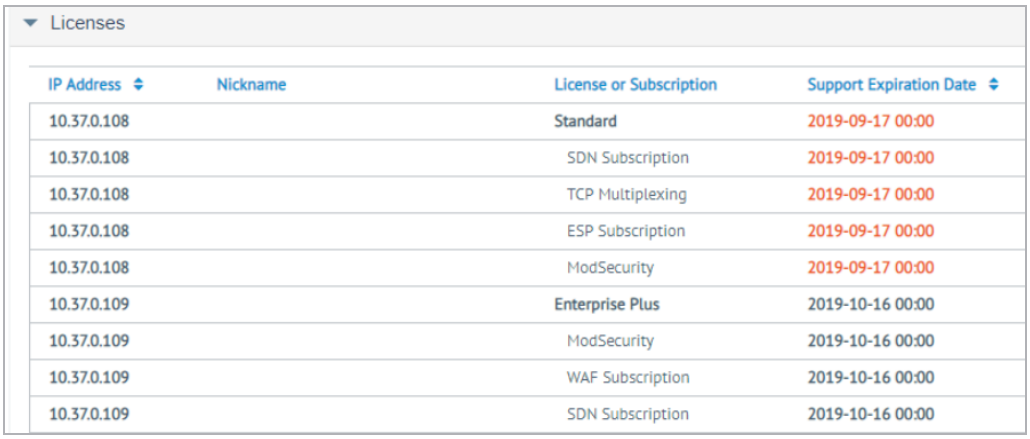
- Yellow: 90 Days

If the device does not have an Enterprise or Enterprise+ subscription, you will only be able to monitor the device because the configuration will be read only.

> If the device has an in-support legacy license, it will have read-write support.

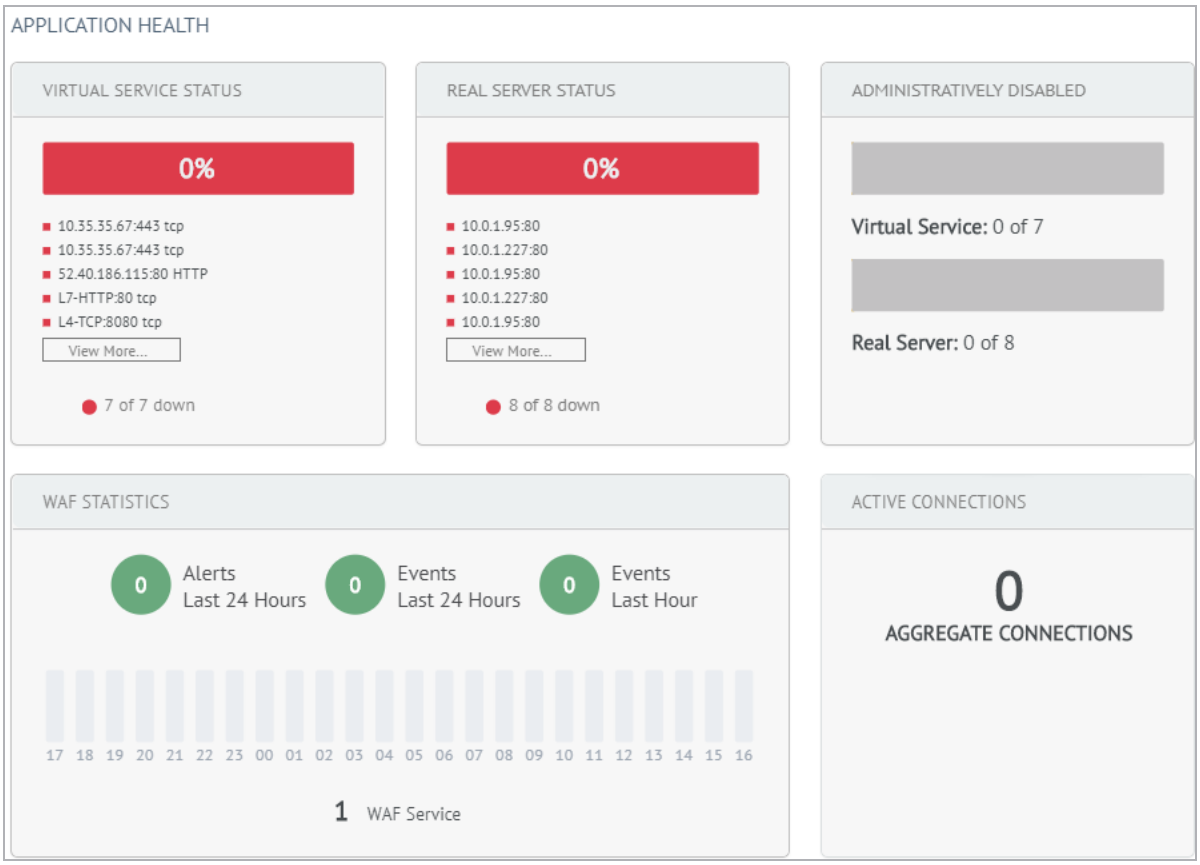
If you click **View List** on the Support Subscription Expiry widget, you can view the Licenses table, which provides information on the type of license and the **Support Expiration Date**. For more information on the Licenses table, refer to the **Licenses** section.

> Licenses and subscriptions that are expired are shown in red in the table.



4.3 Application Health

There are several panels in the **Application Health** section. These are **Virtual Service Status**, **Real Server Status**, **Administratively Disabled**, **WAF Statistics** and **Active Connections**.



A redirect service is always considered up, unless the device on which it is hosted is itself considered down.

- **Virtual Service Status** – This uses a color coding and displays up to five Virtual Servers and five Real Servers. Green indicates the service is up and red indicates it is down. It also displays the number of Virtual Servers that are up out of the total number of Virtual Services. You can click **View More** to open the Monitoring page.
- **Real Server Status** – This panel is similar to the Virtual Service Status panel and displays the same information for the Real Servers.
- **Administratively Disabled** – This panel displays the number of Real Servers and Virtual Services that are administratively disabled (indicated by the yellow color).
- **WAF Statistics** – This panel displays the following:

  - The number of configured WAF services

- The total number of alerts in the past 24 hours (indicated by the triangle at the top of the bar)

- The total number of events in the past 24 hours

- The total number of events in the past hour

- **Active Connections** – This panel displays the following:

  - The total number of active connections aggregated across all managed devices

  - The lowest number of active connections recorded for a single device, across all managed devices

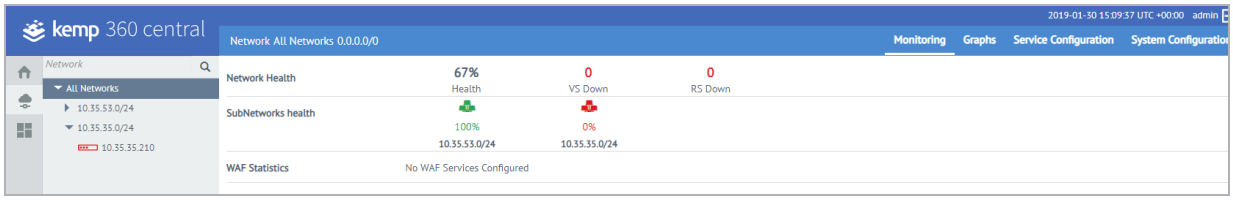
  - The highest number of active connections recorded for a single device, across all managed devices

  - The average number of active connections across all managed devices

If you click the **Active Connections** panel, the **Network Metrics** screen opens.

5 Network and Device Management

This section discusses how networks and devices are managed in Kemp 360 Central. When you click the **Network and Device Administration** icon on the Kemp 360 Central UI, there is a networks area on the left displaying networks and devices.



A network is represented by its IP address, Classless Inter-Domain Routing (CIDR) address, or the nickname specified. It is possible to have a sub-network - this is represented by an indented network. To display status details about all networks, click **All Networks**. To display details on an individual network, click that network.

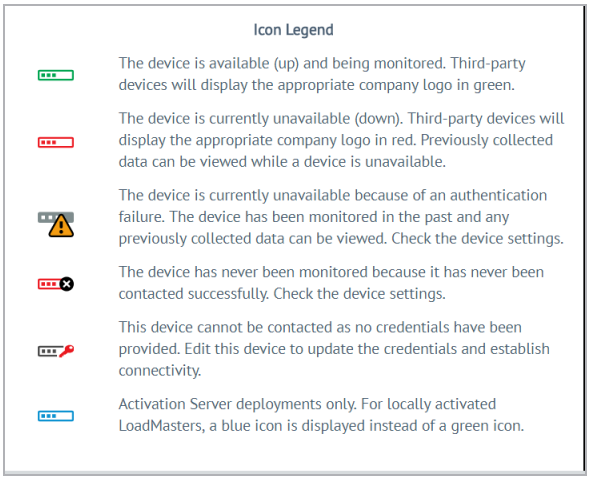
Devices added to a network are represented by an icon underneath the network. If the device was named when it was added, the nickname is displayed, otherwise IP address is shown.

Third-Party device status is represented by the following icons:

Icon	Status
	HA Proxy device is available/accessible
 	HA Proxy device is not available or it is inaccessible
	NGINX device is available/accessible
	NGINX device is not available or it is inaccessible

Icon	Status
	Amazon Web Services (AWS) Elastic Load Balancer (ELB) device is available/accessible
	AWS ELB device is not available or it is inaccessible
	F5 BIG-IP device is not available or is inaccessible
	F5 BIG-IP device is available/accessible
 (spinning)	Device is rebooting

If you want to see what the different icons represent, there is an icon legend at the bottom of the screen (). Roll your mouse over this to view the legend.



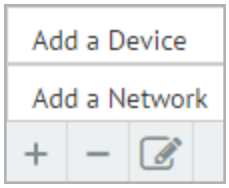
Users should note that selecting a network or device will bring focus to the monitoring and configuration dialogs for the highlighted entity. Please ensure you choose the correct one before adjusting any settings. The term, **Activation Server**, can apply to any device licensed locally by Kemp 360 Central with pooled or metered licensing.

5.1 Network Management

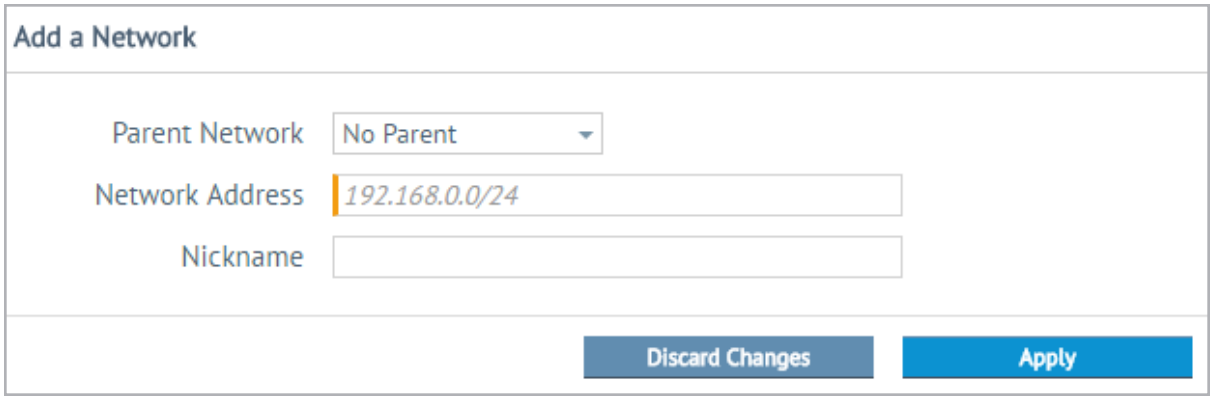
Within Kemp 360 Central, networks are the basic container used to group device instances. You can highlight a network by typing the name of the Network and clicking the **Search** icon. In addition, you can view all available networks by expanding **All Networks**.

5.1.1 Add a Network

1. Click the cloud icon on the left.



2. At the bottom-left, click the plus (+) icon and click **Add a Network**.



3. If creating a top-level network, users should select **No Parent** from the **Parent Network** drop-down list.

4. If this is the first time adding a network using the Kemp 360 Central instance, the **Parent Node** drop-down list does not appear.

5. If adding a subnet, select a parent network from the **Parent Network** drop-down list.

6. Enter a recognizable Nickname for the network.

> Nicknames can only be alphanumeric with hyphens, underscores, dots, and spaces.

7. If no Nickname is entered here the Network's IP address will be displayed everywhere that the Nickname would have been shown.

8. Enter the **IP address** and **CIDR** in the **Network Address** box. The CIDR has a range from 1 to 31.

9. Click **Apply**. A message appears saying the network is added.

5.1.2 Modify a Network

To edit an existing network, select the network on the left and click the pencil icon at the bottom of the screen. Make the changes as needed and click **Apply**.

> If a sub-network or device resides underneath a parent network, do not make any changes to the parent network.

5.1.3 Remove a Network

To remove a network, select a network on the left, click the minus (**-**) icon at the bottom of the screen and click **Remove** on the confirmation pop-up.

> When a network is deleted, all associated subnetworks and/or LoadMasters are also deleted.

5.2 Device Management

Networks constitute the top level of organization in Kemp 360 Central; the devices you add to the networks constitute the second level.

> Kemp 360 Central should only be used to manage LoadMasters that have firmware version 7.1-30b or above installed.

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

> LoadMasters with firmware between 7.1-26 and 7.1-30b have reduced statistics functionality.

> Kemp 360 Central does not work with firmware below 7.1-26.

5.2.1 Adding Devices

This section shows users how to add devices to Kemp 360 Central. Currently supported devices are: Kemp LoadMasters, LoadMaster HA Pairs, ECS Connection Manager, NGINX, HAProxy, AWS ELB, and F5 BIG-IP.

> Once they are licensed against Kemp 360 Central, metered and pooled licensed LoadMasters are automatically added and statistics can be obtained from them.

LoadMasters, like Kemp 360 Central itself, must be licensed to be activated. There are two ways to license a LoadMaster:

- License the LoadMaster by contacting the Kemp license server on the Internet.
- License locally using Kemp 360 Central.

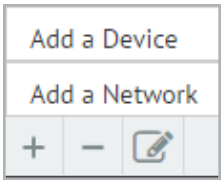
You can add LoadMaster HA pairs that were created on the LoadMaster with Kemp 360 Central as one unit by adding the HA1 and HA2 pair as a shared IP address. The shared IP enables you to more effectively monitor the status and configuration of services across the LoadMaster HA pair. To successfully add a LoadMaster HA pair to Kemp 360 Central, both units must have the same username and password.

> When you add a LoadMaster HA pair to Kemp 360 Central, the shared IP is not included in any statistics.

Before a device can be added to Kemp 360 Central, a network must exist. For steps on how to add a network, refer to the **Network Management** section**.**

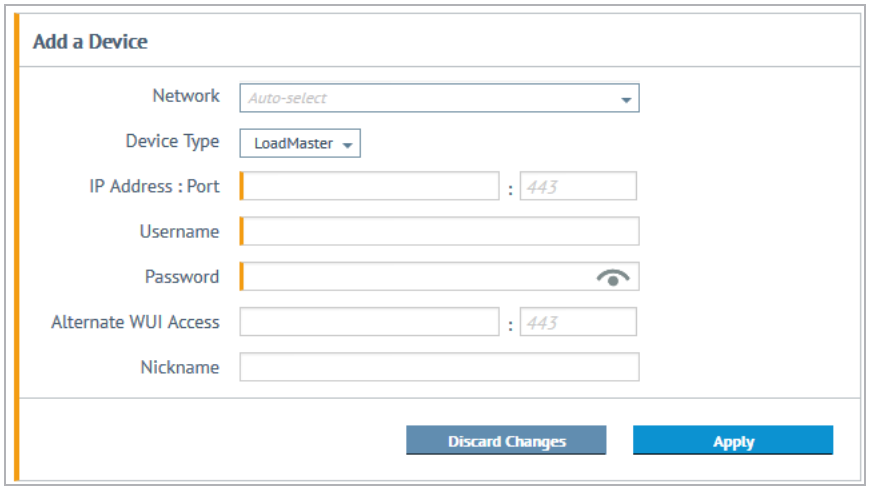
1. Click the cloud icon on the left.

2. Highlight the relevant network. For example: if the device IP address is 192.168.150.10, you must add the device to the network that contains that IP address in its range (as specified by the network's CIDR address).



3. Click the plus (+) icon in the bottom-left and select **Add a Device**.

5.2.1.1 Add Details for a LoadMaster



Use the following steps when adding the details for a pre-licensed LoadMaster:

1. Click the Plus icon at the bottom left of the screen then click **Add a Device**.
2. From the **Device Type** drop-down list, select **LoadMaster**.
3. Type the **IP Address** of the LoadMaster.

> If Network Address Translation (NAT) is being used between your LoadMaster and Kemp 360 Central (for example, your LoadMaster is located in a public cloud), ensure that the IP address in the device settings is the publicly accessible IP address.

The LoadMaster address must be within the IP address range specified for the network you selected in Step 2, or an error is returned.

4. Enter the **Port** number.
5. In a Microsoft Azure environment, type **8443** as the **Port**.

If no **port** is entered, the port defaults to 443.

6. Type the **Username** and **Password** of the LoadMaster.
7. Type the **Alternate WUI Access** address for LoadMasters licensed using local licensing. If you do not specify a port number, it will be auto populated with the private port number.

If using Azure, this is the DNS name that appears in the **Azure Dashboard** screen for Kemp 360 Central.

8. Enter a **Nickname** for the LoadMaster.

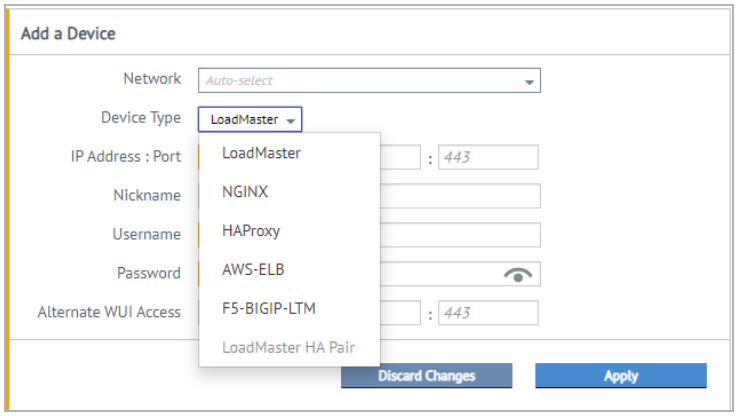
> Nicknames can only be alphanumeric with hyphens, underscores, dots, and spaces.

If a **Nickname** is not entered here, the IP address of the LoadMaster will be used instead.

9. Click **Apply**. A message will appear when the LoadMaster is added.

This will also be seen in the remote logs of the LoadMaster because it will not sync unless the IP address of Kemp 360 Central is public facing.

5.2.1.2 Add Details for a LoadMaster HA Pair



> The **LoadMaster HA Pair** option is disabled if there are less than two available devices.

Before you create a LoadMaster HA pair, you must ensure the following:

- The two LoadMaster HA mode units participating in the HA pair have already been added to Kemp 360 Central as LoadMaster type devices.
- The two LoadMasters are available (up) and communicating successfully with Kemp 360 Central – their icons must be green or blue in the network tree.
- You know the IP addresses and ports of the two HA mode LoadMaster units, in addition to the shared IP address and port.
- Ensure that the credentials (username and password) are the same for both units.

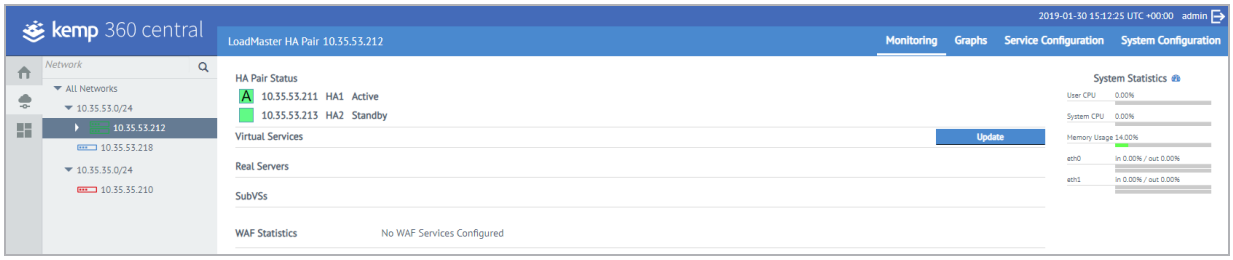
After you ensure the prerequisites shown above are complete, perform the following steps to configure two HA mode LoadMasters into a LoadMaster HA pair:

1. Click the **Network and Device Administration** icon on the left.
2. Click the + icon on the 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	Type the IP address and port of the HA shared IP address used by the HA LoadMasters.
Platform	The platforms available are Hardware / Local Hypervisor, AWS Cloud and Azure Cloud.
Nickname	(Optional) A name for the device that will appear in the network tree on the left and elsewhere in the UI. Nicknames can only be alphanumeric with hyphens, underscores, dots, and spaces.
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 UI's HA Configuration page.
HA2 IP : Port	Select the LoadMaster configured as HA2 in the LoadMaster UI's HA Configuration page.

4. Click **Apply**. The Shared IP Address (or Nickname, if you supplied one) now appears in the appropriate place in the network tree on the left, with the two HA mode LoadMasters organized underneath, as shown in the example below.

> You can perform the same steps on the **Welcome on Board** page.

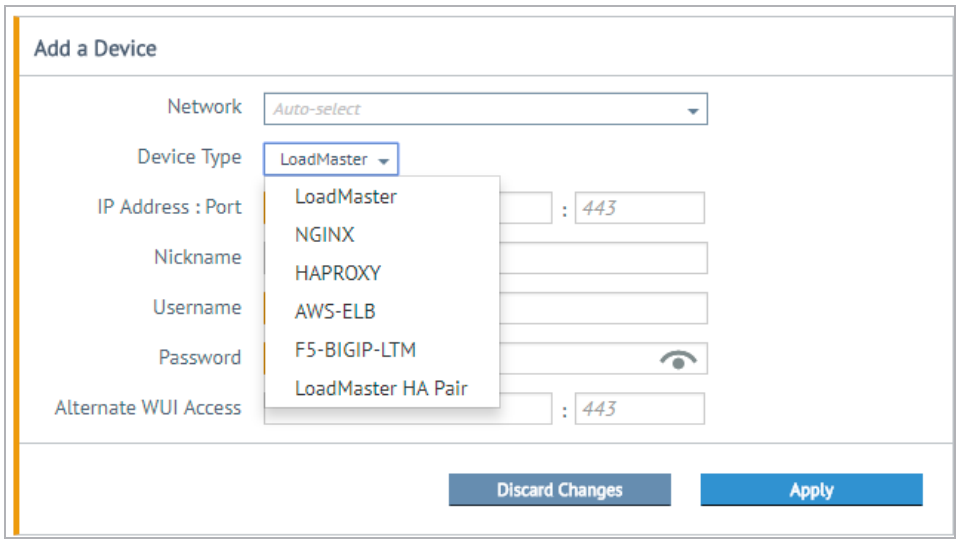


> If you try to create a HA pair with at least one device that has not been contacted by Kemp 360 Central, you will get an error message.

5.2.1.3 Add Details for a Third Party Device

In addition to LoadMasters, Kemp 360 Central enables you to manage third party devices, including NGINX, HAProxy, AWS-ELB and F5 BIG-IP.

The following are the steps for adding a third party device to Kemp 360 Central:



1. From the **Device Type** drop-down list, select the appropriate third party device.

2. The fields available on the screen vary depending on the **Device Type** selected (see the table below). Complete the fields as required. To view tool-tip text for a field, hover the cursor over the field.

3. When finished filling out the fields, click **Apply**.

Field	Description	NGINX	HAProxy	AWS-ELB	F5-BIGIP-LTM
IP Address	The IP address on which the user interface (UI) is available. The address must be within the IP address range of the specified network.	✓	✓	✓	✓
Port	Optional. The port on which the UI is running at the IP address specified. It defaults to 443.	✓	✓	✓	✓
Username/Password	The credentials required to log in to the administrative interface.	✓	✓		✓
Status URI	Required. The path element of a URI that Kemp 360 Central will use to gather status and statistics information from the device (for example, "/status", "/haproxy?status"). The supplied path is appended to the device IP address:port.	✓	✓		
Access Key ID	Required. The			✓	

Field	Description	NGINX	HAProxy	AWS-ELB	F5-BIGIP-LTM
	Access Key ID for logging into the AWS-ELB access key ID				
Secret Access Key	Required. The secret access key for the specified AWS-ELB access key ID.			✓	
AWS LB Name	Required. This name identifies the load balancer on the AWS.			✓	
AWS Region	Required. The AWS region where this ELB is configured			✓	
Alternate WUI Access	Optional. Can be specified as an FQDN or an IP address and port.	✓	✓	✓	✓
Nickname	Optional. Used in the Kemp 360 Central UI as an alias for this. If this is not specified, the IP address and port are used to identify this in the UI.	✓	✓	✓	✓

5.2.1.4 Network Detail Automation

When adding a LoadMaster to Kemp 360 Central, network information is automatically added and configured. Some points about this are provided below:

- If the network does not already exist in Kemp 360 Central, it is added when the LoadMaster is added.

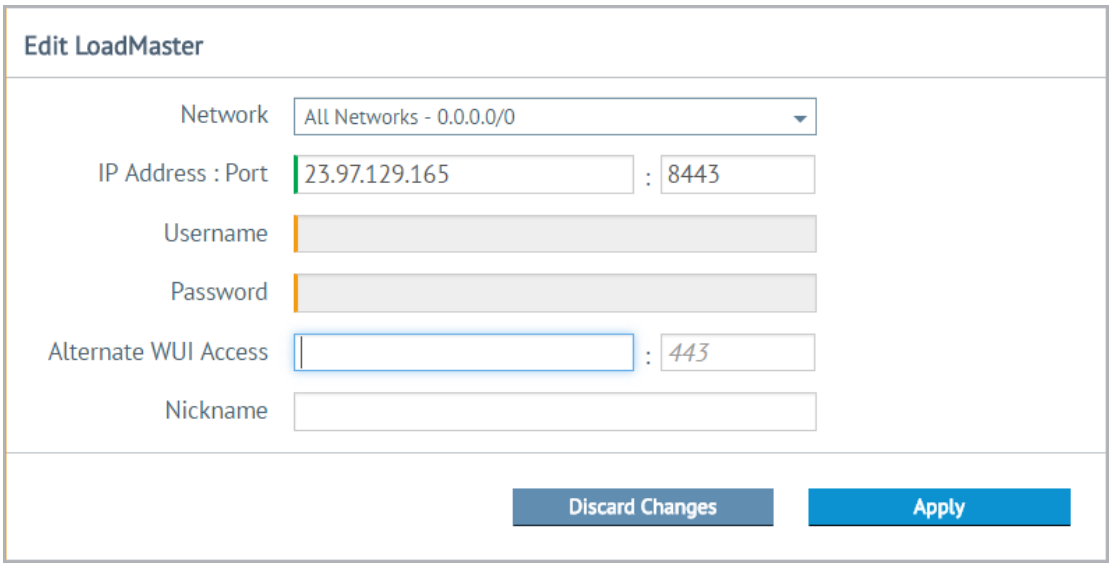
- The LoadMaster is added to the network containing the specified IP address, for example, if a LoadMaster with IP address 10.10.20.20 contains the following networks:
10.10.0.0/16

- 10.11.0.0/16
10.12.0.0/16
The LoadMaster is added to the 10.10.0.0/16 network.

- If the primary network of the LoadMaster is altered (for example, from 10.10.10.20/16 to 10.10.10.20/24), the LoadMaster is moved into the new network.
- Networks automatically organize themselves in the appropriate hierarchy, for example, the network 10.154.0.0/16 automatically becomes a subnet of 10.0.0.0/8 and existing 10.154.n.n/24 networks become subnets of 10.154.0.0/16.
- Networks are not automatically removed if they are no longer present on attached LoadMasters.
- When you add a device with 'All Networks' selected in the Network drop-down, Kemp 360 Central attempts to locate the new device within the network that has the smallest IP address range that contains the specified IP address for the device. For example, you add the following network 13.0.0.0/8. If you then add a device with an IP address that is within that network range, such as 13.0.0.11, Kemp 360 Central places the device within that network. If there are two existing networks that contain the IP address specified, for example, 13.0.0.0/8 and 13.0.0.0/24, Kemp 360 Central locates the new devices under the network with the smaller IP address range (in this case, 13.0.0.0/24).

5.2.2 Modify a Device

To edit an existing device, select the device on the left and click the pencil icon at the bottom of the screen. Make the changes as needed and click **Apply** to apply the changes.



If your initial connection fails and you need to use an alternate address to access the UI, type the address in the **Alternate WUI Access** field and click **Apply**. This is generally applicable in an Azure and AWS environment or if you have configuration problems with your LoadMaster.

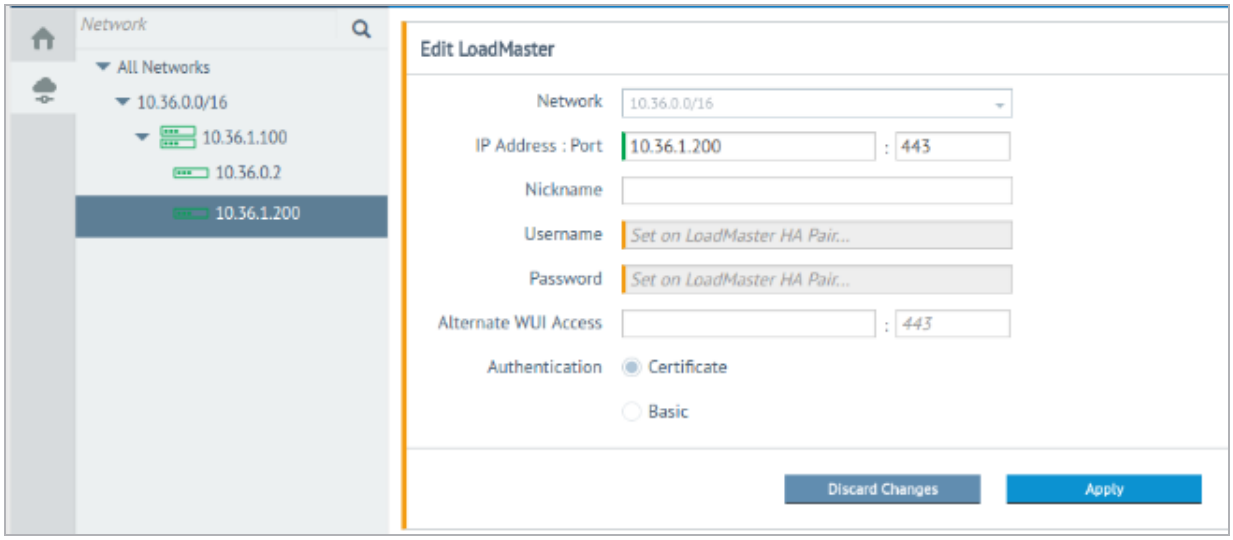
> If certificate-based authentication is being used to authenticate from Kemp 360 Central to the LoadMaster, it may not be possible to edit the **Username** and **Password** for the LoadMaster. For further information, refer to the **Certificate-based LoadMaster Authentication** section.

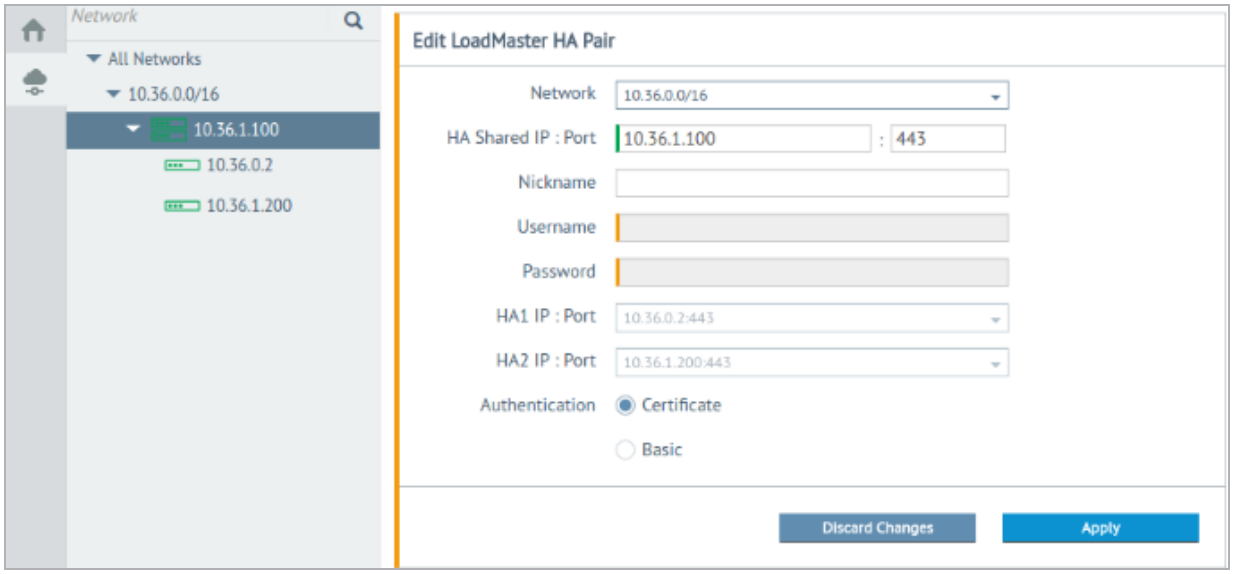
When you modify a device's IP address, the list of networks shown in the **Network** drop-down list only contains networks whose IP address range contains the specified IP address. For example, you have two networks, 10.0.0.0/24 and 192.168.0.0/24, and you modify a device's IP address from 10.0.0.11 to 192.168.0.11. After you do this, only the 192 network appears in the **Network** drop-down list and not the 10 network.

If you are editing a LoadMaster HA pair, you must do it at the shared IP level. In addition, you must ensure that the parameters you provide are valid because they are checked by Kemp 360 Central. Therefore, you must use the correct IP address, correct credentials, and port numbers. If everything is set up and correct, it is verified by the system. If you want to delete a LoadMaster HA pair, you must delete the shared IP address. If you try to delete an individual LoadMaster, you will not be able to.

5.2.3 Modify a LoadMaster HA Pair

You cannot edit the nodes of a LoadMaster shared IP. For example, if the IP address of the LoadMaster HA node is changed for any reason, you can edit the IP address of the node that was changed on Kemp 360 Central. The updated IP address can then be seen on the shared IP in the HA1 or HA2 field. This is shown in the figures below. In the first figure, the individual node is selected and the IP address is updated. The second graphic shows the updated node after the IP was changed.





If you want to move the LoadMaster HA pair to a different sub-network, you can only move it using the shared IP node only.

5.2.4 Remove a Device

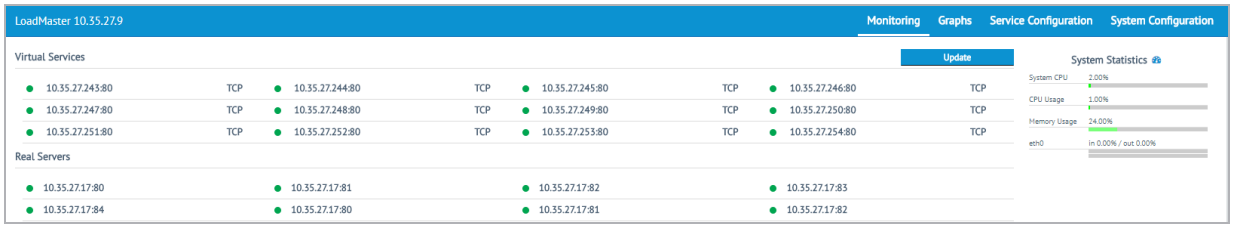
To remove a device, select the relevant device from the left menu. Click the minus (-) icon at bottom-left and click **Remove** when the pop-up message appears. If you remove a shared IP address, it removes the two HA units under it. If you remove a shared IP address that contains locally licensed units, Kemp 360 Central attempts to deactivate both units.

> If you remove a pooled licensing LoadMaster, the license is deregistered, returned to the unused pool, and the LoadMaster enters its grace period.

5.2.5 Checking the Status of a Device

Kemp 360 Central updates the status and configuration information on two separate cycles:

- Status information for devices and services is updated every minute. This is essentially the information displayed on the Monitoring and Graphs tabs, such as availability and statistics.
- Configuration information is updated every 60 minutes. This is essentially the information displayed on the **Services** and **System Configuration** tabs, such as the number of services, SubVSs, Real Servers – and their parameters. You can also request a manual update of a particular device's configuration at any time by following the procedure below.



The status of each device is updated every minute.

> If the LoadMaster does not respond when polled, Kemp 360 Central re-tries the call up to two additional times before marking the device as down. This is to reduce the chance that the failure to poll is because of reasons other than the device not being available (for example, a transient network outage between Kemp 360 Central and the LoadMaster).

To check the current status of an individual device, perform the following steps:

1. Click the **Network and Device Administration** icon.

2. Locate the device whose configuration you want to update in the network tree and click on it. This opens the Monitoring tab for the device.

3. Click **Update** to request an immediate configuration update from the device. A progress bar appears when updating and a message appears informing you that the update was successful. If the device cannot be contacted, this button is disabled.

4. If there are any status changes to your device they will appear here.

> If the update fails, a red warning message appears. To find out more information, you can check the system log.

> The shared IP address of a LoadMaster HA pair does not show up on the **Monitoring** page but the status of the devices does.

5.2.6 Certificate-based LoadMaster Authentication

If you are using a Kemp 360 Central instance with version 1.6 or higher, and you add a LoadMaster with version 7.1.35 or higher, certificate-based authentication is used to authenticate the communications between Kemp 360 Central and the LoadMaster. To enable certificate-based authentication, Kemp 360 Central automatically configures some settings when a LoadMaster is added to it:

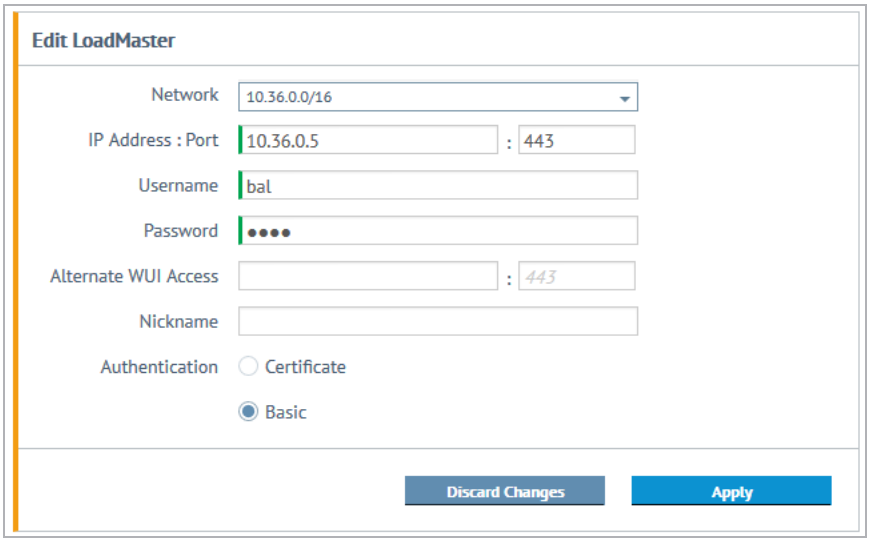
- The Application Program Interface (API) is enabled on the LoadMaster. This is to ensure that Kemp 360 Central can communicate with the LoadMaster.
- Session Management is enabled on the LoadMaster.
- A local user is created on the LoadMaster which is used by Kemp 360 Central to authenticate to the LoadMaster. This user is provided with All Permissions on the LoadMaster.
- A local certificate is generated for the local user created in the previous step. This certificate is then stored in Kemp 360 Central to authenticate to the LoadMaster.
- The **Admin Login Method** on the LoadMaster is changed to **Password or Client certificate**. This is to enable certificate-based authentication on the LoadMaster.

> When a LoadMaster is removed from Kemp 360 Central, none of the above settings change. For example, when you remove a LoadMaster from Kemp 360 Central, certificate-based authentication is not removed from the LoadMaster. It remains

in effect and must be removed manually using the LoadMaster UI, if that is required.

If either the LoadMaster user account or certificate used by Kemp 360 Central is removed from the LoadMaster, or if any of the LoadMaster settings required for certificate authentication listed above are modified, then certificate authentication breaks. This means that Kemp 360 Central will not be able to gather statistics and configuration data from the LoadMaster. To fix this issue, edit the device definition on Kemp 360 Central, change from **Certificate Authentication** to **Basic Authentication**, and re-enter the LoadMaster credentials. This re-establishes contact with the device. After contact is re-established, you can switch back to **Certificate Authentication** if you want.

For more information on user and session management on the LoadMaster, refer to the **User Management, Feature Description** in the LoadMaster documentation.



The workflow is as follows:

1. Add a LoadMaster to Kemp 360 Central using an administrative LoadMaster username and password.

2. Kemp 360 Central attempts to contact the LoadMaster using the credentials supplied. If it is successful, Kemp 360 Central then attempts to set up certificate authentication with the LoadMaster. If certificate authentication fails, you get an error message and see the icon on the device either remain as the 'never contacted' icon (for unmanaged devices) or change to the 'unauthorized' icon. If SMTP is set up correctly, you also receive an email message that certificate authentication has failed.

3. Kemp 360 Central continues to try and contact the device. If negotiating certificate authentication fails and/or contact is never established, you can edit the LoadMaster configuration on Kemp 360 Central so that Kemp 360 Central and LoadMaster will use only basic authentication (username and password) and will not attempt to negotiate certificate authentication. To do this:

a) Click the device in the network tree.

b) Click the Edit icon at the bottom left of the UI.

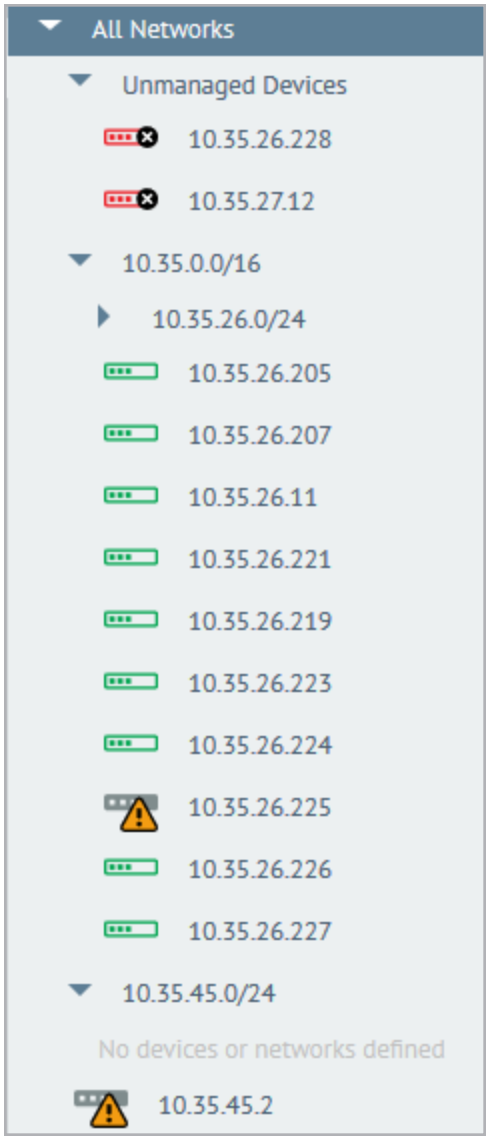
c) Under **Authentication**, click **Basic**.

d) Click **Apply**.

Since version 1.16 of Kemp 360 Central you can now choose to opt out of certificate authentication by editing the **Authentication** setting so that the unit uses basic authentication and does not attempt to establish certificate authentication. To change from **Certificate** to **Basic** authentication, re-enter your username and password for the device, select **Basic** and click **Apply**.

5.2.7 Unmanaged Devices

If there are any devices that Kemp 360 Central has never contacted successfully, these are clearly identified in the left frame in a node entitled **Unmanaged Devices** directly under **All Networks**. In addition, each unmanaged device has a specific icon that is easily recognized. If there are no unmanaged devices present, the **Unmanaged Devices** node is hidden and cannot be seen.



To address issues with Unmanaged Devices:

- Check the credentials required to log into the device and if necessary, edit the device and re-enter it into Kemp 360 Central
- Ensure the device is properly connected to the network
- Check the Kemp 360 Central logs and the logs on the device

When you add a device with **All Networks** selected in the Network drop-down, Kemp 360 Central attempts to locate the new device within the network that has the smallest IP address range that contains the specified IP address for the device. For example, you add the following network:

13.0.0.0/8. If you then add a device with an IP address that is within that network range, such as 13.0.0.11, Kemp 360 Central places the device within that network. If there were two existing networks that contain the IP address specified, for example, 13.0.0.0/8 and 13.0.0.0/24, Kemp 360 Central locates the new device under the network with the smaller IP address range (in this case, 13.0.0.0/24).

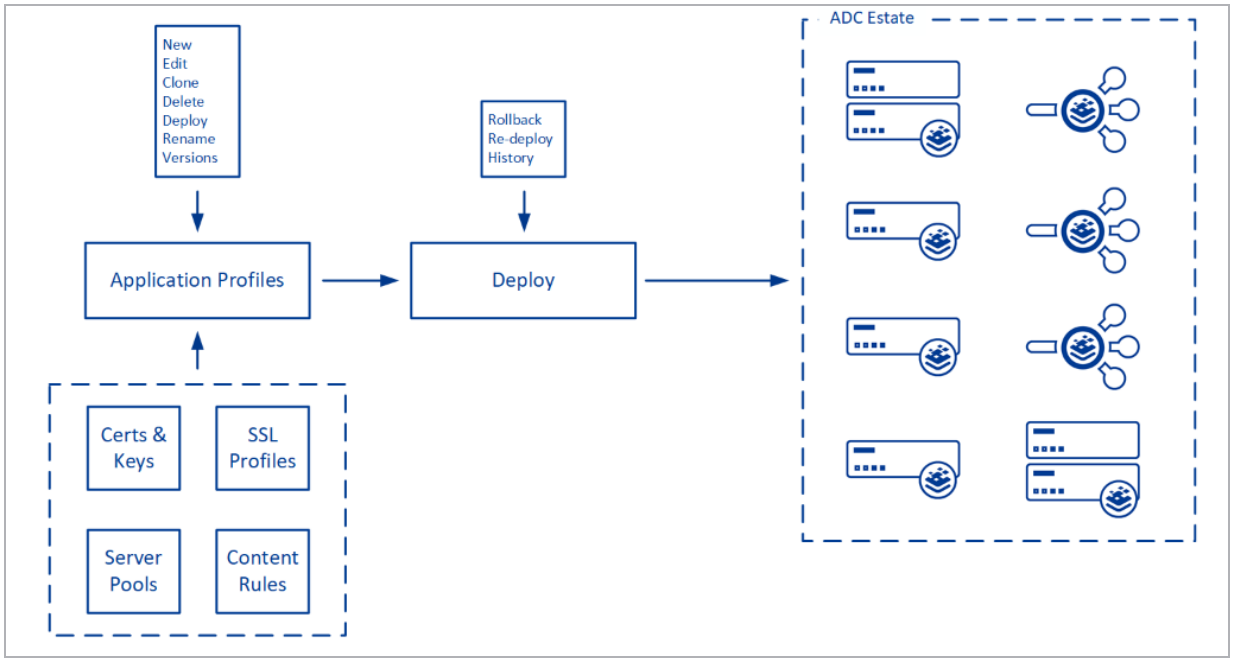
If you add a LoadMaster and give it incorrect credentials, it is added to the Unmanaged Devices section. If you then apply the correct credentials and select **All Networks**, the LoadMaster is added to the correct subnet based on its administration IP address. Where subnets overlap, the smaller of the sub-networks is selected.

6 Application Configuration Management

Kemp 360 Central Application Configuration Management provides centralized control over the creation, maintenance, and deployment of application configurations on LoadMaster load balancing devices. It simplifies and accelerates the task of deploying and updating applications and reduces the risks associated with manual configuration.

6.1 Overview

Application Configuration Management in Kemp 360 Central is based around application profiles that define how an application is load balanced. Application profiles include definitions on the scheduling and persistence to be used in addition to how connections are secured. Application profiles are re-usable, with deployment-specific elements such as server pools and SSL certificates being specified at deployment time.



Application profiles define the Virtual Services (VS) and SubVS required to load balance the application and contain application-specific configuration of parameters such as timeout values and

scheduling methods. Application profiles can also link to pre-defined SSL policies and traffic modification rules to enable centralized management of these elements across multiple profiles. Deployment-specific configurations such as SSL certificate, server pools, and IP addresses are specified when deploying an application profile.

The Deployment History lists each application profile deployment and can be expanded to view details such as the certificate used. To enable rollback of deployments to a known good version or state, any deployment can be redeployed to replace the most recent deployment.

Server pools group application servers to allow for easy re-use and maintenance. They exist independently of application profiles and changes can be applied across all application profiles that reference the server pool.

SSL certificates and private keys are maintained in the certificate repository. Server certificates, certificate chains, and private keys may be uploaded to the system and selected when deploying an application profile. The certificate repository also provides insight on expiring certificates with filtering on 30-day and 90-day expiry timeframes. Use of the certificate repository is optional and certificates and keys may be uploaded for single use at deployment time.

All private keys uploaded to the certificate repository are stored as password protected PEM files. If you do not want to store private keys in Kemp 360 Central, certificates and keys can be specified at deployment and not stored.

6.2 Using Configuration Management

Application Configuration Management (CM) in Kemp 360 Central can address many use cases, all of which enable rapid and consistent configuration of application delivery resources.

DevOPS and Continuous Delivery

With CM, the load balancer configuration can be defined and tested as part of the development process before being made available for production use. Application profile versioning uses the minor version number of a profile to identify if a profile is in 'development' or production ready. If the minor version is zero (for example, 5.0), the application profile is considered production ready and may be deployed by the system or manually. If the minor version is non-zero, the application profile is considered to be in development and can only be manually deployed.

Configuration management enables the rapid creation of disposable environments for development, QA, and staging. This reduces the effort and cost of maintaining and hosting parallel systems.

Multi-Cloud Deployment

In a multi or hybrid cloud environment, configuration management enables consistency across platforms and provides a single point of control. For example, a single application profile can be defined to optimize and secure delivery of services based on the Apache web server. This profile can then be applied across the complete estate of Apache services reducing the configuration and maintenance effort and ensuring consistent deployment.

Hosting Service Provider

Service providers that offer customer-specific application instances can simplify life-cycle management of application resources through the use of pre-defined profiles for the workloads being delivered to users. The use of profiles ensures consistency and accelerates deployment and provides a single point to manage change across all customer instances.

6.3 Application Profiles

Overview

Application profiles are used to define the properties of an applications VS and at least one VS must be defined in a profile. Deployment-specific properties such as IP addresses and certificates are not contained in the profile but instead are provided at deployment.

> You can have up to a maximum of 64 Virtual Services (any combination of Virtual Services and SubVSs) in an application profile.

When updates are made to an application profile, no changes are made to the LoadMaster estate. The profile must be deployed to update the LoadMaster configuration.

You can deploy application profiles to any LoadMaster under management by Kemp 360 Central. When deploying, you can select the target LoadMaster from the drop-down list or you can create a new LoadMaster instance. When creating a new LoadMaster instance as part of an application profile deployment, the system waits until the newly created LoadMaster is contactable before proceeding with deployment.

You can deploy a newly-defined LoadMaster automatically to VMware and KVM environments or manually to any supported platform or cloud.

When deploying a previously deployed application profile (regardless of version), they system will (where possible) auto-populate the application settings from the last successful deployment.

You can roll back deployed application profiles to a previously deployed version by selection any prior deployment and selecting redeploy.

Version Management

Application profiles are assigned version numbers in a *major.minor* format. Minor versions are used when developing and testing a profile and are created by 'Saving' the profile. To create a new major version, 'commit' the profile and the new version will be available for deployment. You can revert to an older major version of an existing profile by going to the **ACTIONS** column and selecting **Versions**. Locate the version you want to restore and click **Restore**.

> You can have as many major versions as you want but you are only allowed one minor version for each profile. You cannot deploy minor versions; only major versions can be deployed.

6.4 Server Pools

While there is no concept of server pools in the LoadMaster, you can define a server pool in Kemp 360 Central that is applied to LoadMaster as individual Real Servers.

When you are creating a server pool, if you want to use the same, or similar, parameters for the next server pool, select the **Remember Parameters** check box. When adding a new server pool, if you select the **Remember Parameters** check box, the fields automatically populate but you can override this if you want. If you have a long list of server pools and you want to find one, you can use the filter. To edit a server pool, go to the **ACTIONS** column and click **Edit**.

Server pools also includes health checks to perform on server pool members. HTTP, HTTPS, ICMP Ping, and TCP Connection health check types are currently supported and are applied to each member of the server pool on deployment. You can select **None** if you do not want to use any health check.

> If you try to delete a server pool that is already deployed on an application profile, you receive an error message.

> You must specify the IP address (FQDN is not currently supported) and the port of each server you are adding to the pool.

6.5 Certificate Repository

The certificate repository is used to store keys and certificates (including intermediate and root certs). The system supports the import of PEM formatted certificates and keys from file or by pasting the PEM encoded certificate/key. The import function supports the import of multiple certificates (for example, a certificate and associated root and intermediated certs) in a single operation. Private keys can also be included in the import file.

It is not possible to import a private key unless there is an associated server certificate in the import file/paste or if the associated server certificate is already in the repository. If you attempt to import a certificate that already exists (based on checksum and subject key identifier), the system will quietly ignore the import but highlight the certificate after import. If you attempt to import a certificate that already exists (based on the subject key identifier), the system will check if the valid-from date on the certificate being imported is later than the existing cert before replacing it.

You can have multiple certificates with the same Common Name (CN). To uniquely identify a certificate, use the subject key identifier or the description. The description allows users to provide custom text to describe the certificate. This is useful to identify entries if the CN is used multiple times.

To view where any certificate is deployed, select the certificate and click the **Usage** tab. This page has a filterable list of all LoadMaster instances where the certificate is deployed and the application profile for the deployment.

Private Key Security

All imported private keys are stored as password protected key files and a password must be provided for every private key imported. This password, known as the 'Deployment Password', will be required at deployment to decrypt the private key.

If you do not want to store the private key on Kemp 360 Central, you can import server certificates without an associated key and the system will prompt for the key file at deployment time.

Certificate Management

You can quickly locate certificates using the filter or you can select the widgets at the top of the screen to quickly identify certificates that have expired, are due to expire within 30 days, are due to expire within 90 days, and due to expire in 90 days or greater.

To view a certificate, go to the **ACTIONS** column, hover over the relevant ellipsis and click **View**. On the left hand pane, a tree appears showing how this certificate occurs in the certificate chain. If you add another certificate in this chain, it updates the hierarchy immediately to show where this new certificate sits.

6.6 Rule Management

Rules are used on LoadMaster to either direct traffic based on content or to modify content. The following rule types are supported

- Content Matching
- Add, Delete, and Replace Header
- Modify URL
- Replace string in response body

For full detail on configuring rules, consult the LoadMaster documentation.

Rules may be used across multiple application profiles.

6.7 Configuration Management - Quick Start

How to Deploy a Non-SSL Application using CM

1. Add a LoadMaster to Kemp 360 Central where you can deploy the application.
2. Create a server pool with a least one application server.
3. Create an application profile with at least one VS.
4. From the application profile listing, deploy the application (click **Deploy** on the **ACTIONS** column).
    a) Select the target LoadMaster from the dropdown list.
    b) For each VS defined, provide an IP address and select the server pool created previously.
5. View the status of the deployed application in the **Deployment History**.

How to Deploy an SSL Secured Application using CM

1. Add a LoadMaster to Kemp 360 Central where you can deploy the application.
2. Create a server pool with a least one server.
3. Create an application profile with at least one VS.
4. Select **Security** and enable **SSL Termination** in the Virtual Service properties.

5. Deploy the application from the application profile listing (click **Deploy** on the **ACTIONS** column).

6. Select the target LoadMaster from the dropdown list.

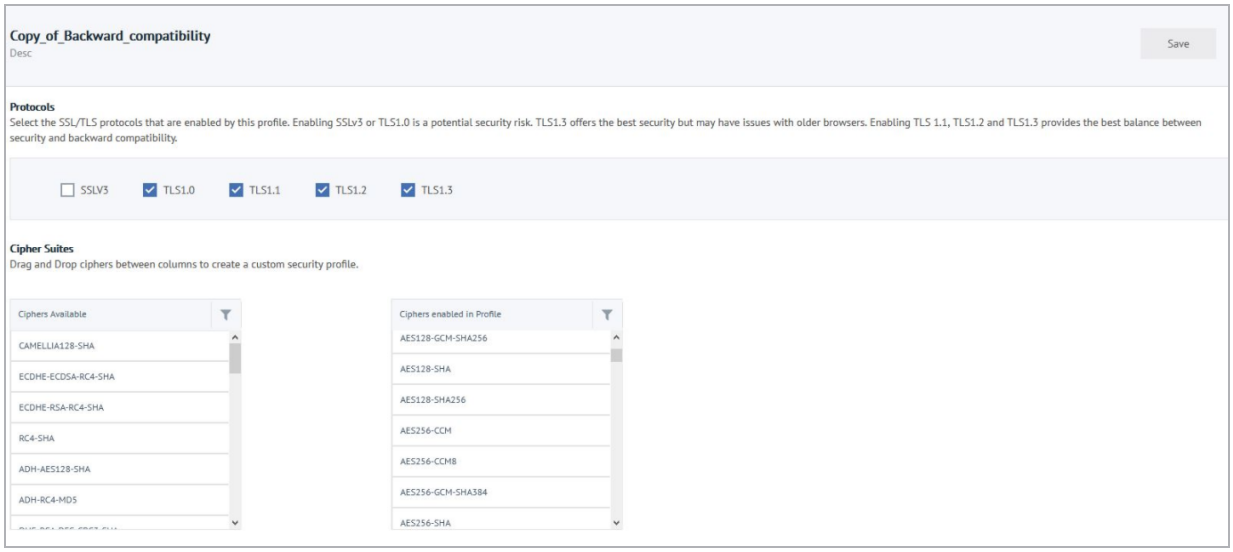
7. For each VS defined:

    a) Provide an IP address and select the server pool created in Step 2.

    b) Upload the certificate and key in a single PEM encoded file.

6.8 SSL Profiles

Within the **Configuration Management** section, you can create SSL profiles.



SSL profiles allow you to define ciphers and protocols to be used and allowed. When configuring application profiles you can use these SSL profiles to reduce time to deploy in addition to automating and standardizing application profiles to security best practices.

6.9 Deployment Scripting

Deployment scripting is a way to script and use LoadMaster features that have not yet been added into the Kemp 360 Central UI. You can view the deployment scripts when deploying an application profile.

You can use deployment scripting to configure the following features because they are not available in the Kemp 360 Central UI:

- ESP
- WAF
- Various advanced features not available in the UI

> Refer to the **Kemp 360 Central Deployment Scripting Technical Note** on the Kemp Documentation page for details on the syntax and parameters to use in deployment scripts.

7 LoadMaster Deployment

Kemp 360 Central supports the creation and deployment of Virtual LoadMaster Machines (VLM) to simplify and accelerate the process of making licensed LoadMaster instances available for use.

VLMs can be created as standalone devices or as Highly Available (HA) pairs. After the VLM is defined, it can be deployed directly to VMware and KVM hypervisors or downloaded as a virtual machine image for manual deployment. After a VLM is deployed, it can be configured to load balance applications by deploying application profiles or by manually configuring services.

7.1 LoadMaster Deployment Limitations and Prerequisites

- LoadMaster deployments are supported in VMware 6.0, KVM, XEN, and Hyper-V hypervisor environments.
- You must be logged in as the **admin** user to use the feature of LoadMaster deployment. While other users can view the status of deployments, they cannot create or deploy virtual machines.
- The **Automated Deployment** feature does not work in either Internet Explorer or Microsoft Edge. When you try to activate a LoadMaster against Kemp 360 Central from the LoadMaster UI using either of these browsers, you get an error.
- The deployed LoadMaster must be able to communicate with Kemp 360 Central to maintain its license.
- The LoadMaster must be running version 7.2.48.1 and above.
- Both HA and non-HA deployments are supported.

7.2 Create the LoadMaster Virtual Machine

To create a new application profile, click the **Configuration Management** icon, expand the **LoadMaster Deployment** section, and click **Create LoadMaster**. Then, click **Create LoadMaster VM**. Type the name of the LoadMaster and provide a profile description. Click **Create**. You can select either a standalone LoadMaster or a HA pair. There are a number of fields that you must then complete as follows:

- **Default Gateway**
- **LoadMaster 'bal' Account Password**
- **DNS Server #1**
- **Eth0 IP Address / CIDR**

  CIDR specifies the number of bits in the subnet mask. Set the CIDR to /24 for subnets with a mask of 255.255.255.0. Additional interfaces may be added by clicking the **plus** icon.

- **Port** (the **VLAN ID** field is optional).

The license capacity options available for the Virtual Machine depend on the license and subscription applied to Kemp 360 Central. Re-licensing is supported if the capacity demands change in the future. A summary of the profile is displayed after you click **Next**. You can then select whether you want **Automatic Deployment** or **Manual Deployment**.

7.3 Virtual Machine Deployment

LoadMaster Profiles are deployed by opening the **Configuration Management > LoadMaster Deployment > Create LoadMaster** page. Selecting a profile that is in the **Ready** or **Downloaded**

states, and clicking the **Deploy** button. You can deploy a LoadMaster either automatically or manually.

Automatic Deployment enables you to provide the parameters required to instantiate a VLM using a specific deployment profile on a specific hypervisor platform (IP address, credentials, and so on). In addition, Kemp 360 Central manages the VLM instantiation directly with the hypervisor platform.

> Automatic deployment is currently supported for VMware vCenter, VMware ESXi, and KVM hypervisors only.

Manual Deployment of a LoadMaster profile enables you to download a pre-configured VLM image (or pair of LoadMaster VLMs configured into HA) that you can then manually install on a wider range of hypervisor platforms. VLM images can be manually deployed to:

- VMware (vCenter or ESXi)
- Hyper-V (Gen1 image only)
- VirtualBox
- KVM
- Xen

As with automated deployment, the manual deployment process can be entered at the end of the deployment profile creation process; it can also be entered by going to the **LoadMaster Virtual Machines** screen, selecting a **Ready** or **Downloaded** profile from the list, and clicking **Deploy**.

General Deployment Notes

An SSL certificate validation error may be observed in the Kemp 360 Central log during either a manual or automatic deployment, and a similar error may be observed in the hypervisor log. This may be caused by a difference between the date and time settings on Kemp 360 Central and on the target hypervisor environment. The deployment will still succeed, but the result is that Kemp 360 Central will not be able to communicate with the LoadMaster using certificate authentication until the time on the hypervisor is later than the time that the LoadMaster image was created on Kemp 360 Central. If this happens, you can temporarily go back to **Basic Authentication** by editing the device definition on Kemp 360 Central. In general, ensure that all hypervisor environments being used for automatic and manual LoadMaster deployments have their date and time set properly (ideally using NTP) to avoid SSL certificate validation errors when deploying a profile.

7.3.1 Manual Deployment

To manually deploy a LoadMaster, select the hypervisor format you want to download then follow the on-screen instructions.

> The **VMware ESXi** hypervisor should only be chosen when deploying to a standalone ESXi server that is not being managed by VMware vCenter. If you are deploying to a VMware ESXi server that is being managed by vCenter, then choose **VMware vCenter** as the hypervisor and deploy through vCenter. If you instead select **VMware ESXi** to deploy to an ESXi server that is managed by vCenter, then after deployment you may need to manually adjust the resource settings on vCenter to reflect the datastore to which you deployed the VLM image. This is due to communications/permissions issues between vCenter and ESXi.

Review the profile summary and ensure you are satisfied with the settings.

> Be careful that you do not instantiate a deployment containing the same IP address of one that is already deployed on your network.

After you download the deployment, the status of the LoadMaster profile changes to **Downloaded**. If it is not deployed in a target environment in 7 days, the status changes to **Deploy Error**. Deploy the profile image in the appropriate environment. Refer to the documentation for the selected hypervisor and to the VLM installation guide for the appropriate hypervisor on the Kemp Documentation Page.

Once the downloaded image is added to the hypervisor and is successfully contacted by Kemp 360 Central, it is shown as a blue icon device in the left frame tree and the profile status in the **LoadMaster Deployments** screen changes to **Deployed**.

7.4 Set up the Target Environments

A target environment is the hypervisor environment to which you deploy a LoadMaster profile. When you are using automated deployment, you specify the IP address and credentials used to log in to the hypervisor, as well as platform-specific parameters required to instantiate a virtual machine within that hypervisor environment.

As an optional step during automated deployment, you can save the hypervisor information specified to a named target environment that will be saved for future use. Existing target environments are displayed in the **Target Environment** dropdown for automated deployments, so you can select the saved deployment instead of specifying all the parameters again.

All existing saved target environments are listed on the **Configuration Management > Target Environments** screen in the UI, and all operations on target environments can be initiated from this page.

To set up and view target environments outside of the deployment process, navigate to **Configuration Management > LoadMaster Deployment > Target Environments**. Click **Create New** and complete the details as required.

To edit a target environment, select the target environment and click **Edit**. To delete the environment, select the target and click **Delete**. Click **Delete** again on the confirmation message that appears. You can select multiple environments by selecting the check box next to the **Name** field.

7.4.1 Prerequisite for VLM Auto-Deployment to VMware vCenter or VMware ESXi

Kemp 360 Central makes use of VMware content libraries when automatically deploying a VLM to a VMware vCenter or VMware ESXi environment. Content libraries are commonly used to deploy machines on VMware. When Kemp 360 Central connects to VMware vCenter or VMware ESXi, it attempts to do the following:

- Select a content library associated with the datastore that was specified during the deployment workflow
- Create a new library item in the content library
- Upload the VLM manifest and disk image files to the library item
- Instantiate a VLM using the data in the library item

The VMware vCenter or VMware ESXi datastore that is chosen for deployment (either by specifying one manually during deployment or by choosing an existing target environment) must have an existing **Content Library** defined on it, or the deployment will fail with an error in the Kemp 360 Central Debug and Audit logs that looks like this:

```
ERROR Could not fetch library for target 'target-environment-name' to deploy
'profile-name' (Library not found).
```

If you see this error after a failed deployment, you can work around it by manually creating a content library on the VMware vCenter or VMware ESXi datastore. The name of the library does not matter (Kemp 360 Central picks the first one it finds on the datastore) and it can be empty.

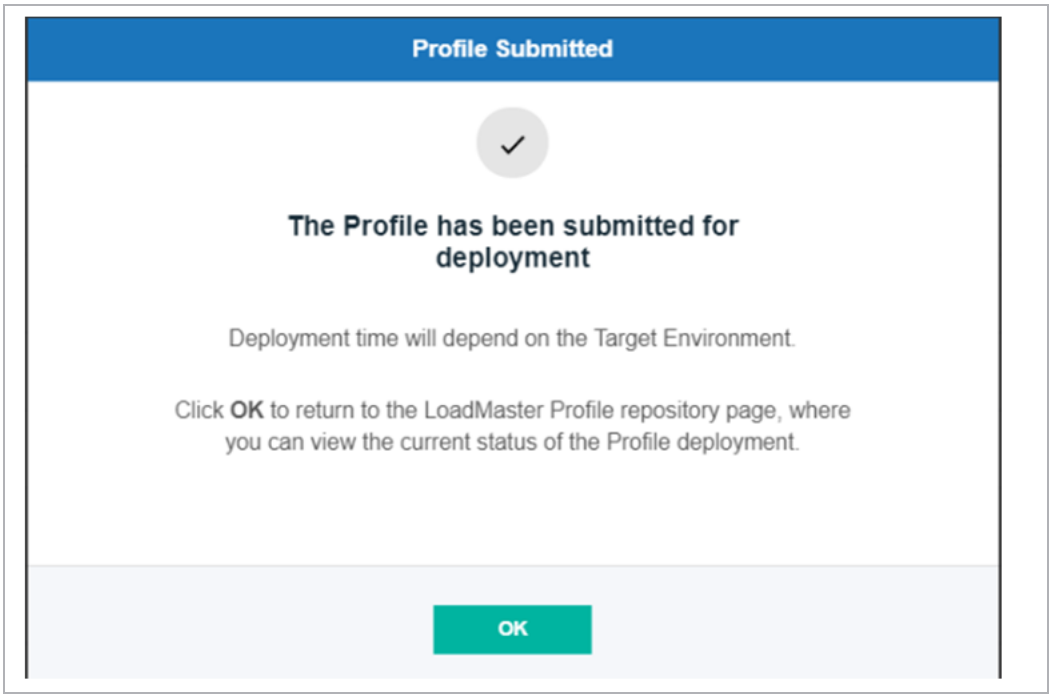
For more information on VMware content libraries and how to create them, see the VMware documentation section Using Content Libraries.

7.4.1.1 Automatic Deployment Procedure for VMware vCenter and VMware ESXi

To deploy VMware vCenter or VMware ESXi using the automated process, click **Automatic**. Choose either to create a new environment or choose an existing target environment from the drop-down.

If you do not select an existing environment, you can enable the **Save as new Target Environment** check box if you want to save the target environment parameters you supply here for later use in another deployment. Complete all the required fields.

> The **VMware ESXi** hypervisor should only be chosen when deploying to a standalone ESXi server that is not being managed by VMware vCenter. If you are deploying to a VMware ESXi server that is being managed by vCenter, then choose **VMware vCenter** as the hypervisor and deploy through vCenter. If you instead select **VMware ESXi** to deploy to an ESXi server that is managed by vCenter, then after deployment you may need to manually adjust the resource settings on vCenter to reflect the datastore to which you deployed the VLM image. This is due to communications/permissions issues between vCenter and ESXi.



After the profile is submitted for deployment and you click **OK**, you are redirected to the **LoadMaster Virtual Machines** screen where you can see the status of your profile, which now appears as **Deploying**.

When the status changes to **Deployed**, the LoadMaster is added to the network tree and the color changes to blue (to indicate this is a metered or pooled licensing device).

If there is an error, the status changes to **Deploy Error** and the icon stays red. You can then check the **Deployment History** for messages recorded during deployment from the hypervisor and Kemp 360 central.

7.4.2 Prerequisites for KVM Auto-Deployment

Ensure that the following capabilities exist on the KVM hypervisor and the unit on which it is hosted before you attempt to automatically deploy LoadMasters to KVM:

1. The host server on which KVM is running must have login through the SSH protocol enabled so that the KVM user specified as part of the credentials for a Target Environment on Kemp 360 Central can securely communicate with the KVM host server. See the documentation for your host operating system for instructions on enabling SSH.

2. Public key authentication is used to authenticate Kemp 360 Central to the KVM host over SSH, so Kemp 360 Central's public key must be added to the list of **Authorized Keys** in the KVM user profile for the user login specified as part of the credentials for a Target

Environment on Kemp 360 Central. When you deploy a LoadMaster to KVM, or when you create a KVM Target Environment, Kemp 360 Central's public key is displayed as part of the user interface (as shown in the procedure below). See the KVM documentation for information on adding the Kemp 360 Central public key as an authorized key to a KVM user profile.

3. The KVM user that is specified in the login credentials for a Target Environment on Kemp 360 Central must have the proper permission to communicate with the **libvirtd** daemon running on the KVM hypervisor. Generally, on a Linux system, you would add this user to the **libvirtd** group. See the KVM documentation and the documentation for your host operating system for instructions on how to give this user permission to communicate with the **libvirtd** daemon.

4. The **netcat** software must be installed on the KVM host server. See the documentation for your host operating system for instructions on installing software packages.

7.4.2.1 Automatic Deployment Procedure for KVM

To deploy KVM using the automated process, click **Automatic** and complete all fields as required.

After your profile is submitted for deployment and you click **OK**, you are redirected to the **LoadMaster Virtual Machines** screen where you can see the status of your profile, which now appears as **Deploying**.

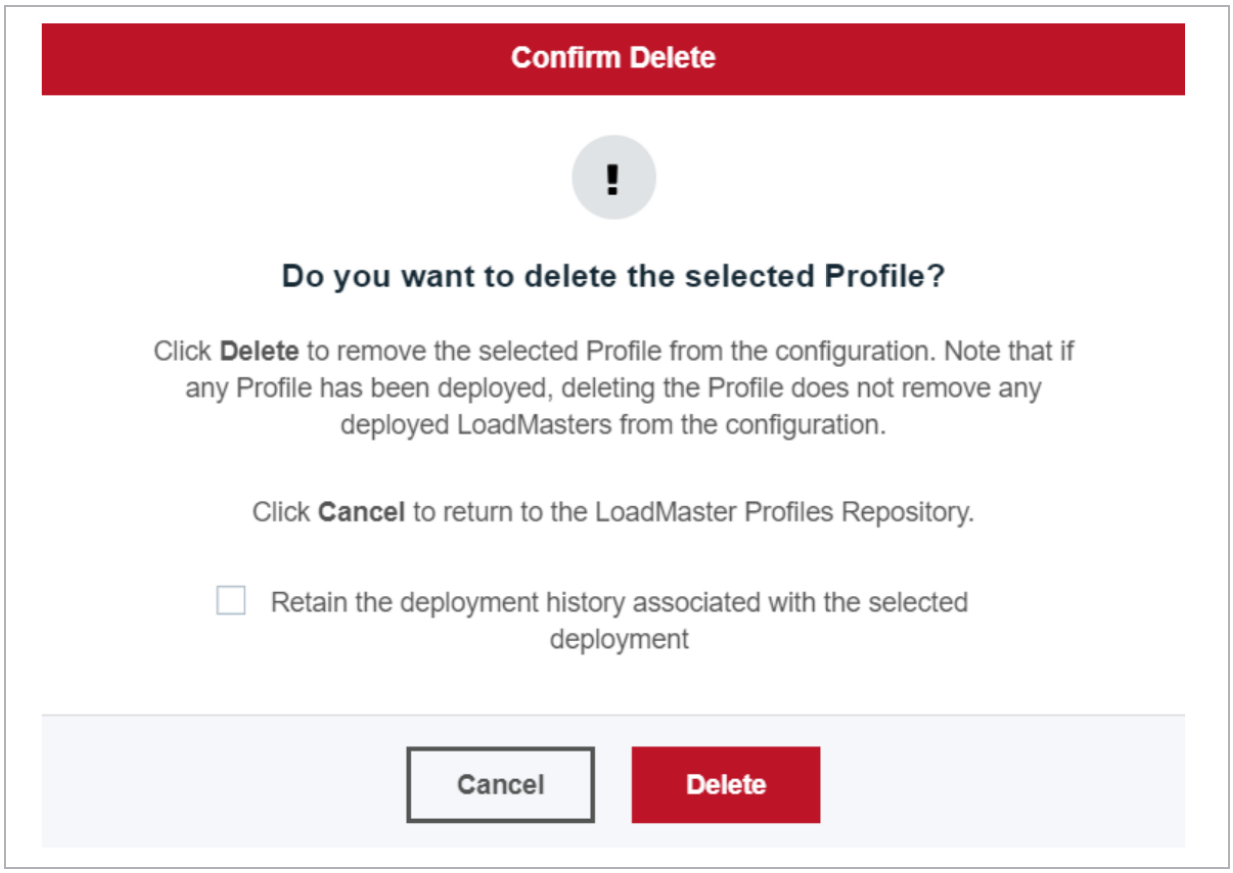
When the status changes to **Deployed**, the LoadMaster is added to the network tree and the color changes to blue (to indicate this is a metered or pooled licensing device).

If there is an error, the status changes to **Deploy Error** and the icon stays red. You can then check the **Deployment History** for messages recorded during deployment from the hypervisor and Kemp 360 central.

7.5 Delete a LoadMaster Profile

To delete a LoadMaster profile, open the **Configuration Management > LoadMaster Deployment > Create LoadMaster** page of the UI, select any profile that is in the **Ready** state, and click the **Delete** button.

The following confirmation screen is displayed:



If you want to retain the deployment history associated with the selected deployment, select the check box. You can delete multiple profiles at the same time by selecting the profiles and clicking **Delete**.

> If you select multiple profiles for deletion, all deployment histories for those profiles are deleted.

7.6 Deployment History

The **Deployment History** screen displays all the messages that are generated by Kemp 360 Central or received from the hypervisor during the automated deployment process. After you auto-deploy a LoadMaster profile, you can view details such as whether the deployment was a success or failure.

> The **Deployment History** does not display any information for manually deployed (downloaded) deployments.)

To view the deployment history, click **Configuration Management > Deployment History**. By default, the table is sorted in reverse chronological order (newest entries first).

To view any deployment messages, click the arrow on the left next to the **Profile Name**. If there is an error, it is displayed in the message. Kemp 360 Central messages are formatted appropriately. Messages returned from the hypervisor are shown unformatted as received from the hypervisor.

To delete a record, click the arrow on the left of the **Profile Name** then click the delete icon.

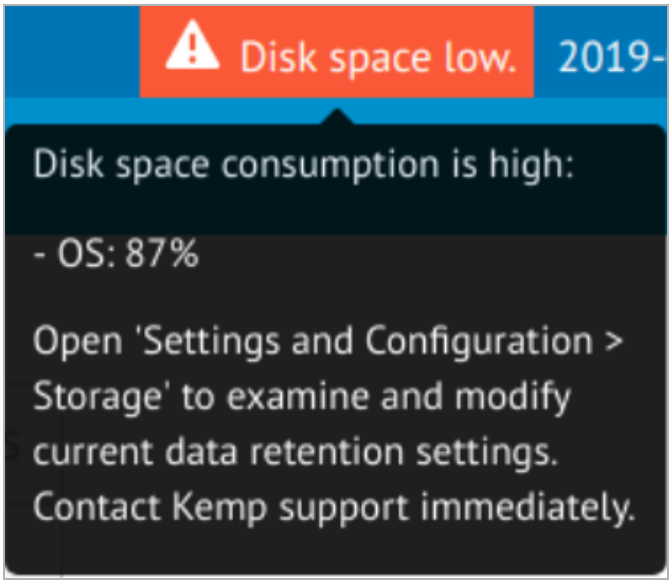
8 System Configuration

It is possible to manage LoadMasters using the Kemp 360 Central interface. To access the LoadMaster configuration area, click the cloud icon in the menu on the left and then select the **System Configuration** tab.

The **System Configuration** section of Kemp 360 Central enables users to locally manage LoadMasters. Users may manage: templates; firmware; reboots; backup; restore and/or syslog settings for any LoadMaster on a network.

Disk Space

A daemon is run every 30 minutes to look at your disk space.



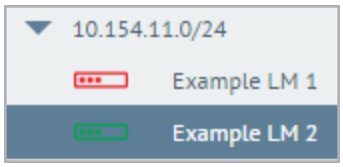
Depending on your configuration, if your system has a single OS partition, there are two critical limits that are set, one by the system and the other is configurable (see **Storage**). The system critical disk alert is triggered if the disk space equals or exceeds 95% of the total disk space available. If this occurs, a notification appears on the UI alerting you of this and it is essential that you contact Kemp Support. In addition, an email containing the same information is also sent to the list of recipients configured in the **SMPT Settings**. The audit log is also updated with this information.

If you have two partitions (OS and data), there is a separate critical threshold for the data partition (this is not configurable). If the data partition exceeds 95% usage, you will see the alert on the UI and be notified by email if your email address is configured in the **SMTP Settings**.

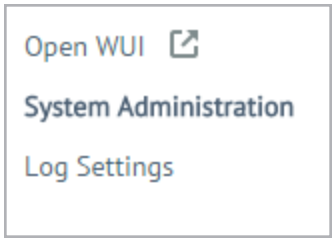
> The UI warning remains displayed, and notifications are sent every 30 minutes until the available amount of disk space is increased by Kemp Support, so that normal system operation can continue. If disk space consumption continues to increase, Kemp 360 Central eventually stops collecting statistics and log data from managed devices.

8.1 Open the LoadMaster UI from Kemp 360 Central

Clicking the Open UI link will open a browser window to the LoadMaster UI. The read-only user does not have access to the **Open WUI** link. To click the **Open WUI** link, follow the steps below:



1. Select the relevant LoadMaster on the left.
2. Click **System Configuration**.



3. Clicking the **Open WUI** link in the menu will open the UI of the selected LoadMaster.

8.2 LoadMaster Reboot

Kemp 360 Central gives users the ability to centrally reboot LoadMasters. You can reboot a single LoadMaster or up to 13 selected LoadMasters simultaneously.

> When Kemp 360 Central issues a reboot command to a device, no other operations (for example, taking a backup) are allowed until the device reboots and is available again.

Reboot a LoadMaster using the Kemp 360 Central interface by following these steps:

1. Click the relevant network or subnetwork in the left pane of the UI.

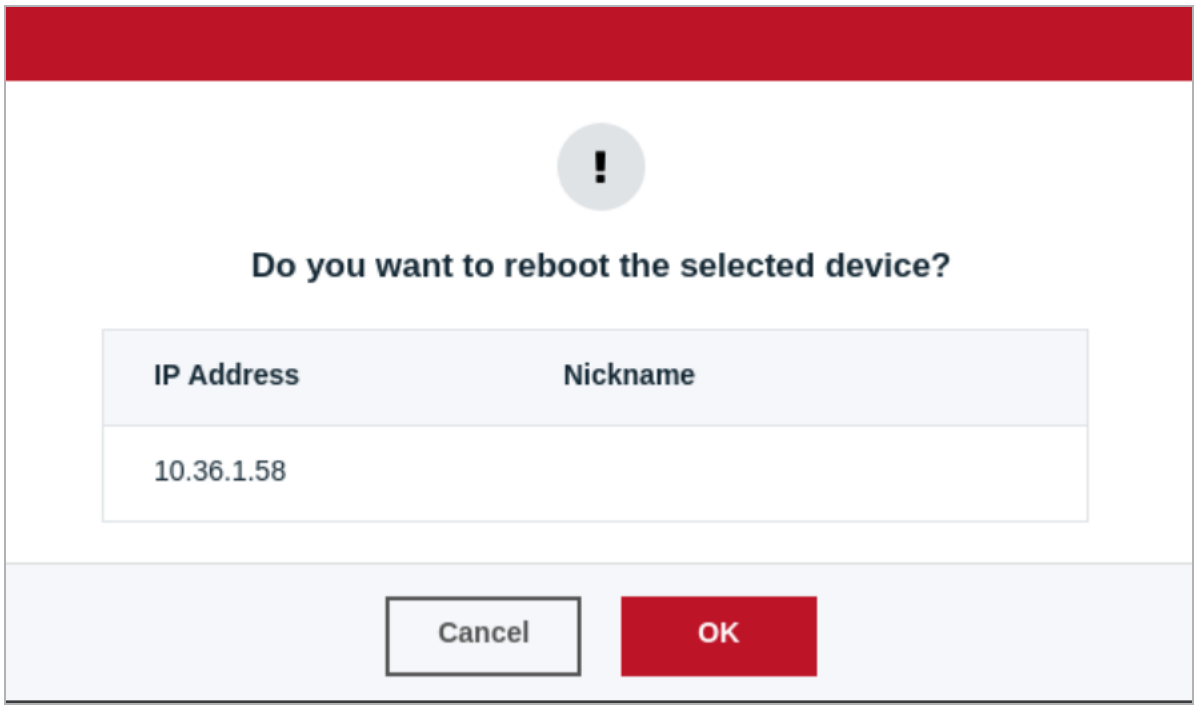
2. In the right pane, select the **System Configuration** tab and then expand the **System Reboot** section.

This displays a list of the LoadMasters on the network you selected in the previous step, as shown in the example below.

3. To reboot a single LoadMaster, select the check box beside the LoadMaster for rebooting and click the **Reboot** button.

4. Reboot up to a maximum of 13 LoadMasters by selecting the check box of each LoadMaster and then clicking the **Reboot** button. Alternatively, select the **Select All** check box to select up to 13 devices on the screen.

> If you select 13 different devices on different pages, you can deselect all devices by clicking **Reset**. In addition, you can use the **Search** field to quickly locate the devices you want.



5. Click **OK**.

6. The system displays **Rebooting**… next to each rebooted unit until the unit is available again.

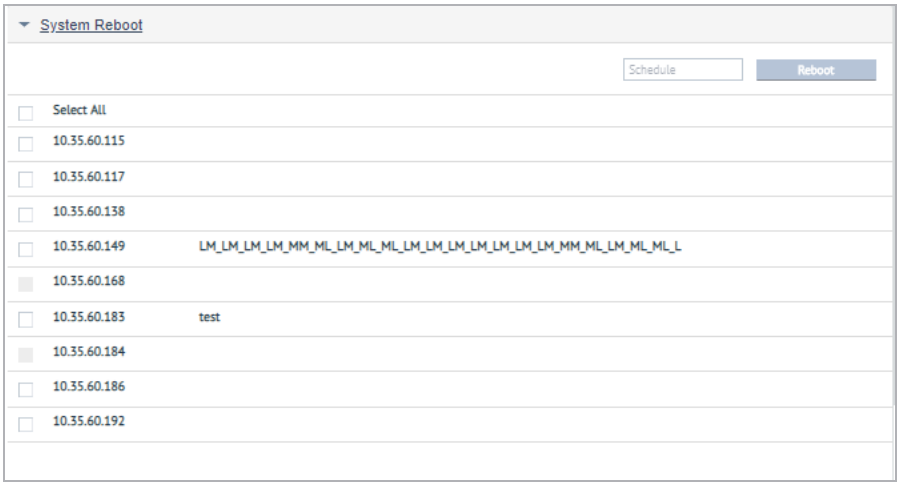
> If your LoadMasters are in a HA configuration, you can reboot them using the shared IP address or directly from the devices.

8.2.1 Schedule a LoadMaster Reboot

By carrying out the following steps, users can schedule the reboot of a single or multiple LoadMasters:

1. Click the cloud icon on the left of the screen.
2. Select the **System Configuration** tab.

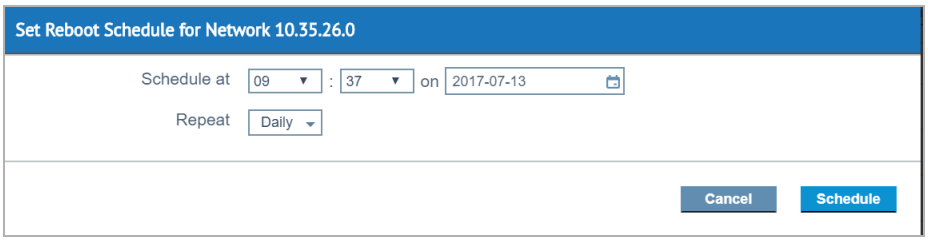
3. In the left-hand menu, click the network to which the LoadMaster or LoadMasters you wish to schedule for a reboot is attached.



4. Expand the **System Reboot** section.

5. Select the check box of the LoadMaster or LoadMasters you wish to reboot and click the **Schedule** button.

If you wish to schedule a reboot of all LoadMasters in a network, enable the **Select All** check box.



6. Enter the time, date and frequency, for which you wish to schedule the reboot.

> Tasks cannot be scheduled within one hour of each other.

7. Click **Schedule**.

8. Further information on scheduling can be found in **Scheduled Actions**.

8.3 Template Management

Using a template automatically populates the settings in a Virtual Service. This is quicker and easier than manually configuring each Virtual Service. If needed, changes can be made to any of the Virtual

Service settings after using the template.

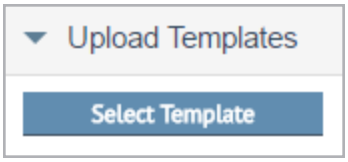
For more information on templates, please refer to **Virtual Services and Templates, Feature Description**.

To add a template to a LoadMaster using Kemp 360 Central, the template file must first be uploaded to the Kemp 360 Central Global Repository.

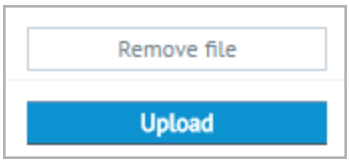
8.3.1 Upload the Template to Kemp 360 Central Global Repository

To do this, use the following steps:

1. In the menu, click the **Global Repository** icon and then click **Template Management**.



2. Click **Select Template**.
3. Browse to and select the template file. Multiple files can be selected, if desired.

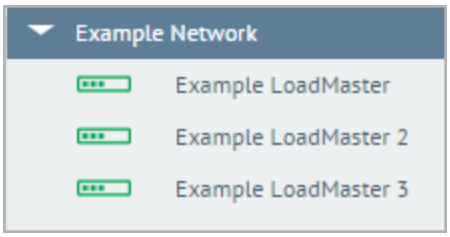


4. Click **Upload**.
5. Wait for the template file to finish uploading. A message appears when the upload completes.

8.3.2 Upload a Template File to a LoadMaster

Once you have uploaded a template to Kemp 360 Central, the template can be installed on one or more LoadMasters. To do this, perform the following steps:

1. Click the cloud icon on the left of the screen.
2. Select the **System Configuration** tab.



3. In the left pane, select the relevant network or LoadMaster.

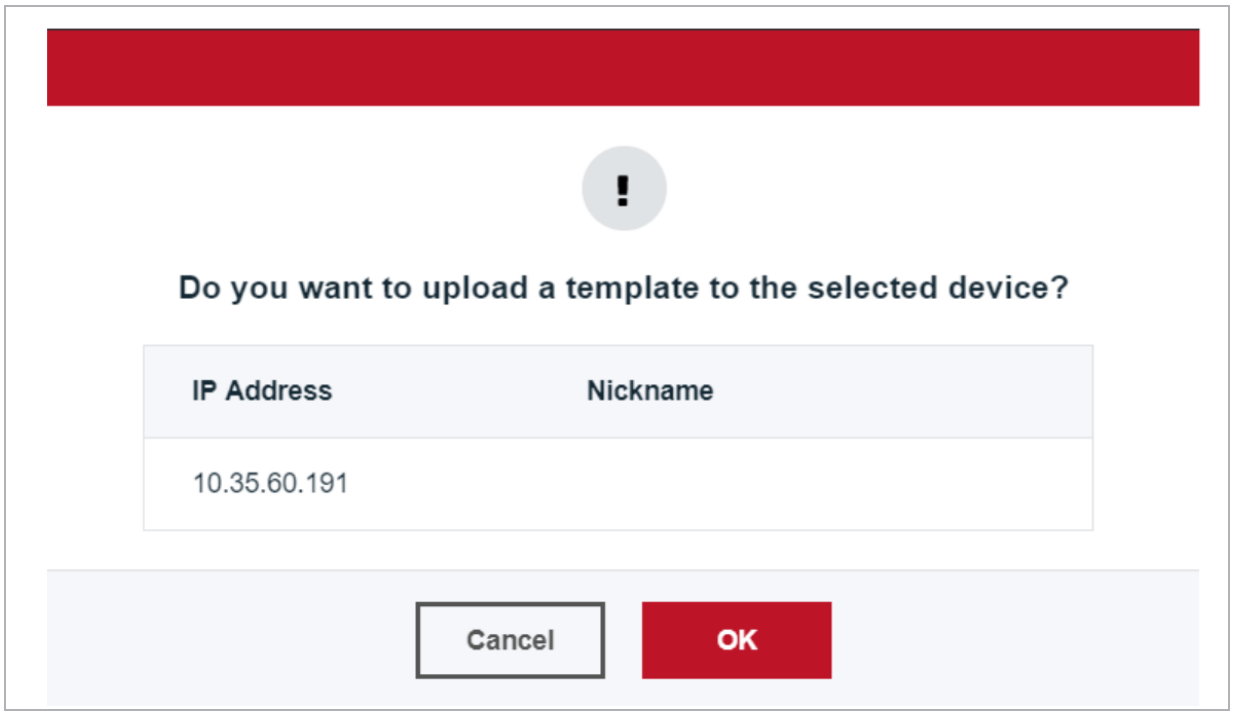
4. In the right pane, expand the **Templates** section.

If you selected a network instead of a LoadMaster, you can select up to a maximum of 13 LoadMasters and install a template on them all at one time.

5. From the **Select a template to apply** drop-down menu, click the template you wish to add.

6. Do one of the following:

- If you have multiple templates selected over different pages, you can click **Reset** to reset your selection.
- If you selected a single LoadMaster in Step 3, click **Upload Template** to install the template on that LoadMaster.
- If you selected a network in Step 3, select the LoadMasters on which you want to install the template, and then click **Upload Template**.



7. Click **OK**.

> On systems where there are a large number of LoadMasters, you can only select a maximum of 13 LoadMasters to update at one time. In addition, you can use the **Search** field to quickly locate the devices you want.

8. A message appears when the upload completes.

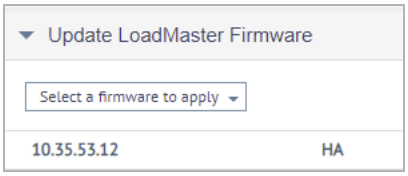
8.4 Update the LoadMaster Firmware

To update the LoadMaster firmware using Kemp 360 Central, first upload the firmware update file to Kemp 360 Central Global Repository. Then, the desired LoadMasters can be updated with the selected firmware. Firmware updates can be immediate or scheduled for a future date, time and frequency.

8.4.1 Upload the LoadMaster Software Update File to the Global Repository

To do this, follow the steps below:

1. In the menu, click the **Global Repository** icon and then click **LoadMaster Software Updates**.



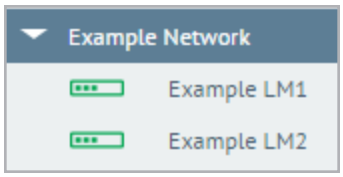
2. Click **Select Software**.
3. Browse to and select the firmware update file. Multiple files can be selected, if desired.
4. Click **Upload**.
5. Wait for the firmware update file to finish uploading.
6. A message appears when the upload completes.

8.4.2 Update the Firmware on Selected LoadMasters

When the firmware has been uploaded to Kemp 360 Central Global Repository, LoadMasters can be updated individually or in groups (up to a maximum of 13 LoadMasters). To do this, follow the steps below:

> The LoadMaster will be automatically rebooted after the firmware update has completed. This may result in a brief service outage. If possible, perform upgrades during a maintenance window or during known periods of reduced traffic.

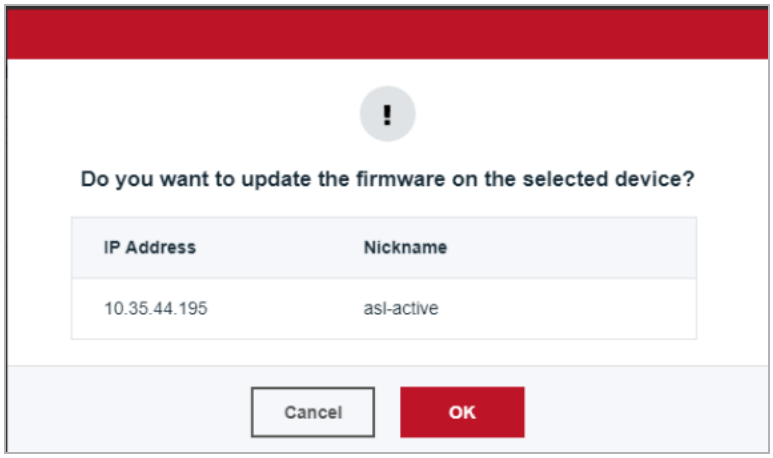
1. Click the cloud icon on the left of the screen.
2. Select the **System Configuration** tab.



3. Select either an individual LoadMaster, or a network - depending on whether you want to update an individual LoadMaster or multiple LoadMasters on a network. You can select a maximum of 13 devices to update at one time. If you have multiple devices selected over different pages, you can click **Reset** to reset your selection.

For LoadMasters configured in HA Pairs, you can only schedule an upgrade on the individual LoadMasters in the pair, and not using the HA Shared IP address.

4. Click **Select a firmware** to apply to display the list of available firmware updates.
5. Click the desired firmware version.
6. If a network was selected, select the check-box(es) of the LoadMaster(s) to be updated.
7. Click the **Update Firmware** button.



A warning displays if the firmware version being installed is lower than the current LoadMaster firmware version. This may result in a loss of some functionality.

LoadMasters with firmware between 7.1-26 and 7.1-30b have reduced statistics functionality.

Kemp 360 Central does not work with firmware below 7.1-26.

8. Click **OK** to proceed.

9. Wait for the firmware update to complete.

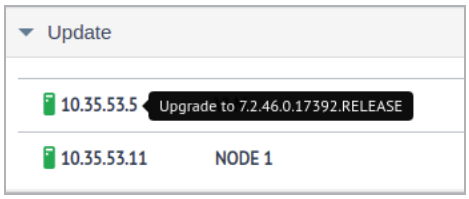
When the update is finished, the LoadMaster automatically reboots,

When the LoadMasters come back online, Kemp 360 Central reflects their current status.

8.4.3 Schedule a LoadMaster Firmware Update

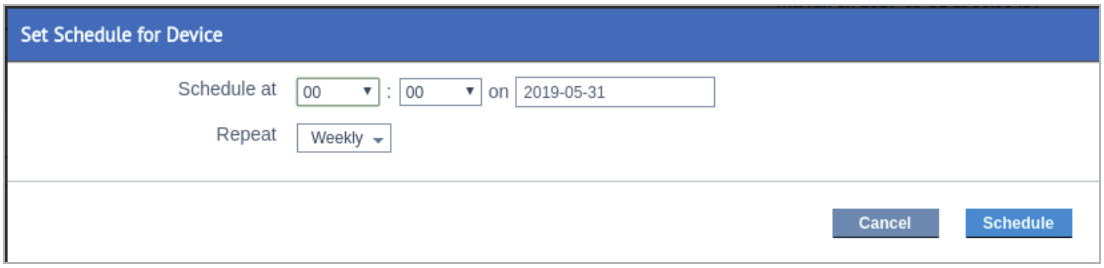
By carrying out the following steps, users can schedule the firmware update of one or multiple LoadMasters:

1. Upload the LoadMaster firmware update file, as described in the **Upload the LoadMaster Software Update File to the Global Repository** section.
2. Click the cloud icon on the left of the screen.
3. Select the **System Configuration** tab.
4. In the left-hand menu, select the relevant network.



5. Expand the **Update LoadMaster Firmware** section.
6. Select the check box of the LoadMaster or LoadMasters you wish to update the firmware of and click the **Schedule** button.

If you wish to schedule a firmware update of all LoadMasters in a network, select the **Select All** check box.



7. Enter the time, date and frequency, for which you wish to schedule the firmware update.

Tasks cannot be scheduled within one hour of each other.

8. Click **Schedule**.

Further information on scheduling can be found in the **Scheduled Actions** section.

8.5 Backup/Restore

Kemp 360 Central allows users to create a backup archive, store that backup centrally on Kemp 360 Central, and restore that backup archive onto any LoadMaster.

To restore the settings, a backup file must first exist in Kemp 360 Central.

There are two ways to take a backup. The method to use depends on whether the LoadMaster to be backed up exists in Kemp 360 Central:

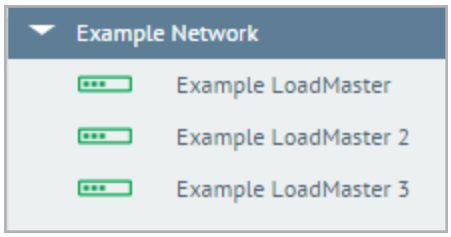
- If the LoadMaster exists in Kemp 360 Central: back up using Kemp 360 Central - refer to the **Back up a LoadMaster and/or SSL Certificates using Kemp 360 Central** section for steps on how to do this.
- If the LoadMaster does not exist in Kemp 360 Central: back up using the LoadMaster UI and upload the backup file to Kemp 360 Central. Refer to the **Importing a LoadMaster Backup into Kemp 360 Central** section for steps on how to do this.

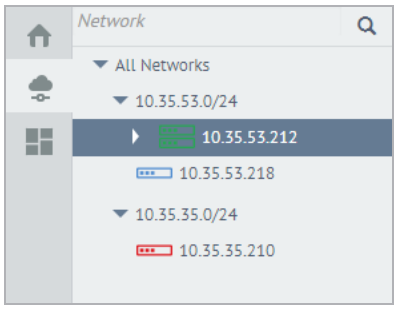
8.5.1 Back up a LoadMaster and/or SSL Certificates using Kemp 360 Central

LoadMasters that exist in Kemp 360 Central may be backed up in the following way:

> LoadMaster profiles and target environments are included in all backup archives and are restored when a backup archive is applied.

1. In the Kemp 360 Central UI menu, click the cloud icon.

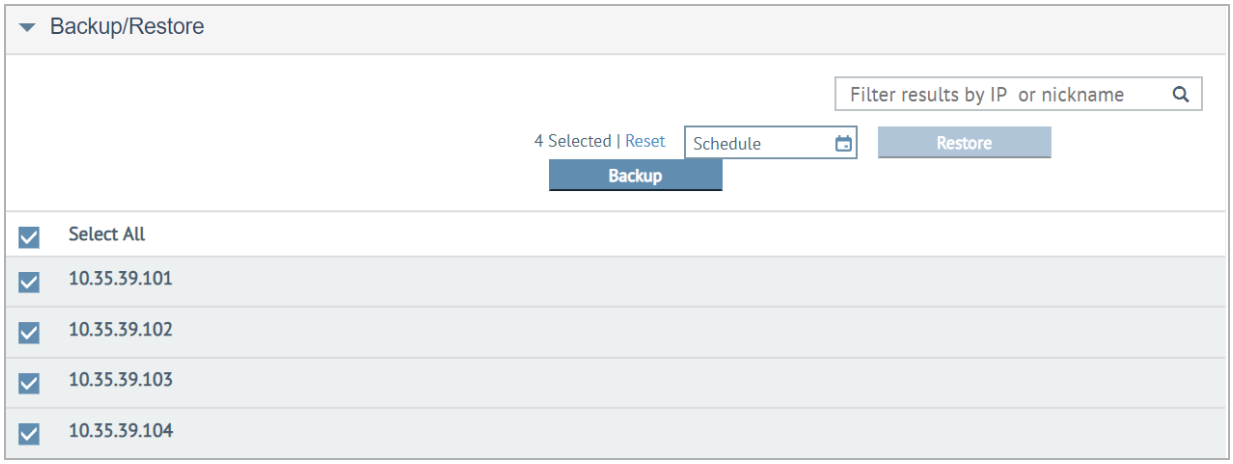




2. Select a network (as shown in the first image), to backup multiple units. To back up a single unit, navigate to that unit in the network tree (as shown in the second image).

3. Select the **System Configuration** tab.

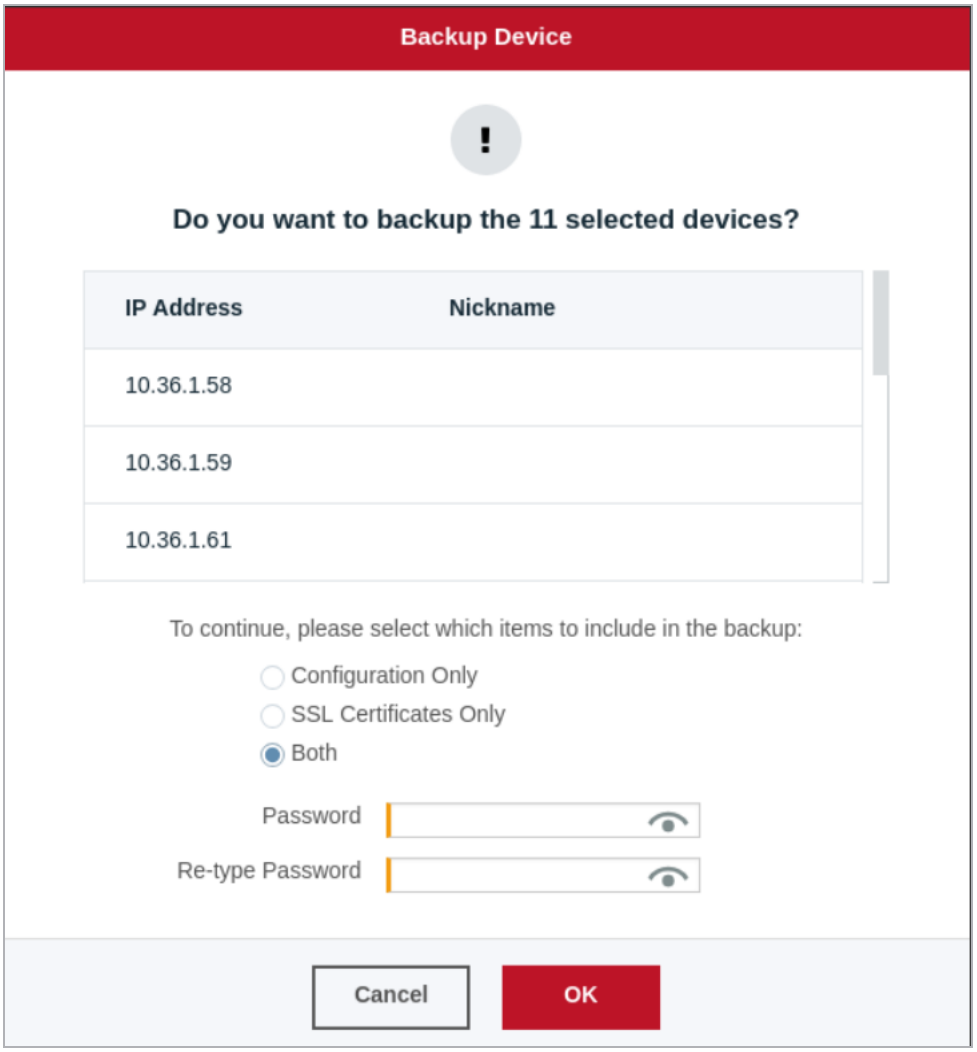
4. Expand the **Backup/Restore** section.



5. Select the LoadMasters that you would like to back up. You can select the **Select All** check box to select a maximum of 13 LoadMasters.

> On systems where there are a large number of LoadMasters, you can only select a maximum of 13 to back up/restore at one time. In addition, you can use the **Search** field to quickly locate the LoadMasters you want. If you have multiple LoadMasters selected over different pages, you can click **Reset** to reset your selection.

6. Click **Backup**.



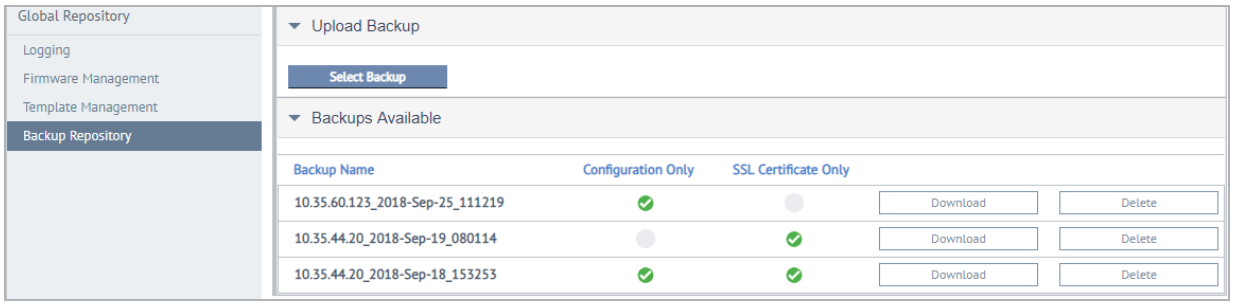
A pop-up message appears with three options:

- **Configuration Only**: Select this option to back up your LoadMaster configuration only.
- **SSL Certificates Only**: Select this option to back up your SSL certificates only.
- **Both**: Select this option to back up both your LoadMaster configuration and SSL certificates.

> All backups are password-protected, so you will be prompted for a password that will be required upon restore. If you select **SSL Certificates Only**, an additional password is required for the certificate archive.

If you select **SSL Certificates Only**, an additional password will be required for the certificate archive.

7. Select the option you want.
8. Click **Confirm**. A pop-up message displays saying the backup was created.



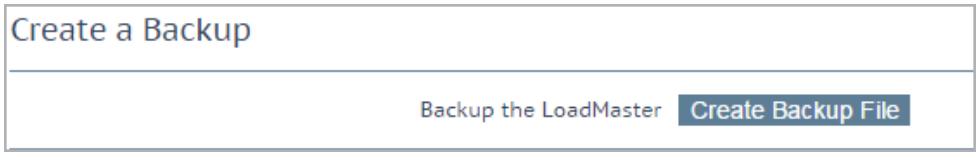
After you create the backups, the backup files can be found in the **Backup Repository** section of the **Global Repository**. The downloaded zip file contains a configuration archive, a certificate archive, or both. These can be extracted from the zip file and applied to a LoadMaster outside of Kemp 360 Central, using either the LoadMaster UI or the LoadMaster API.

A configuration-only backup archive, downloaded to the customer's local machine from either the LoadMaster or Kemp 360 Central, can be uploaded to Kemp 360 Central. This is recognized as a LoadMaster backup and can be restored to any LoadMaster. Any other file uploaded to the backup repository of Kemp 360 Central is also stored and labeled as a configuration-only backup archive. However, if the customer attempts to restore one of these to a LoadMaster, they get an error. This is true for all of the following files that might be uploaded to Kemp 360 Central:

- An SSL archive that was downloaded from either the LoadMaster or Kemp 360 Central.
- A combined configuration and SSL backup archive that was downloaded from Kemp 360 Central.
- Any random file that is not a backup archive (for example, an image file, a text file, and so on).

8.5.2 Importing a LoadMaster Backup into Kemp 360 Central

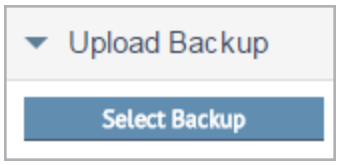
For LoadMasters that do not exist in Kemp 360 Central, you can create a backup locally using the LoadMaster UI, and then upload it to Kemp 360 Central.



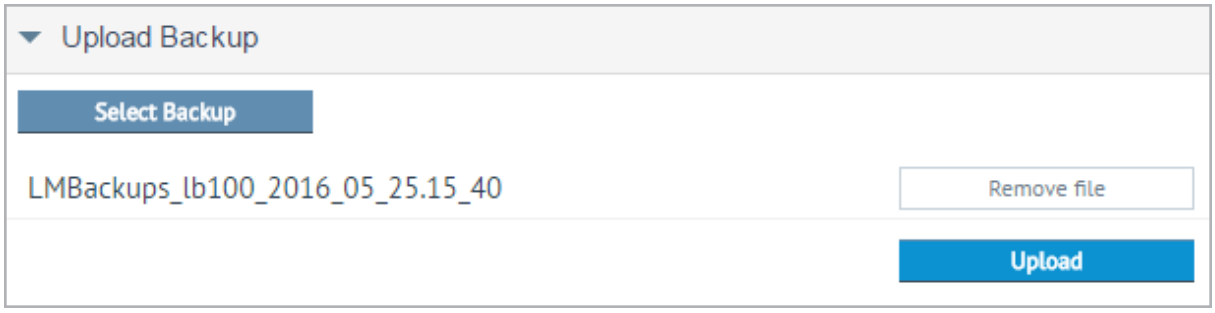
In the UI of the LoadMaster, go to **System Configuration > System Administration > Backup/Restore > Create Backup File**.

Then, upload the backup file to Kemp 360 Central by following the steps below:

1. In the Kemp 360 Central UI menu, click the **Global Repository** icon and then click **Backup Repository**.



2. Click **Select Backup**.
3. Browse to and select the relevant backup file.



4. Click **Upload**.
5. Wait for the backup file to upload.

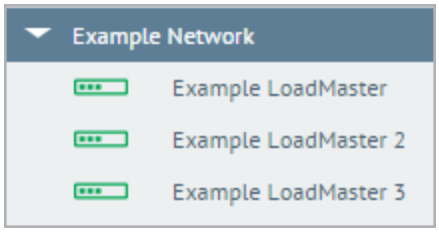
A message will appear when the upload completes. The upload is now available for applying to LoadMasters under Kemp 360 Central control using the Restore backup functionality as described in the **Restore LoadMaster and/or SSL Certificate Settings** section.

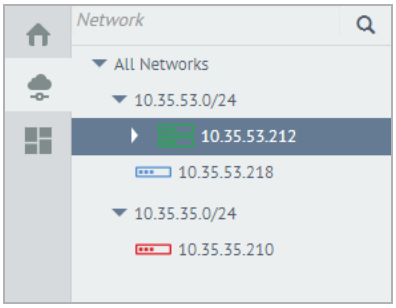
8.5.3 Restore LoadMaster and/or SSL Certificate Settings

When a backup file is available in Kemp 360 Central, the settings can be restored to a LoadMaster.

> Please do not restore a non-Azure LoadMaster backup to an Azure LoadMaster

1. Click the cloud icon on the left of the screen.



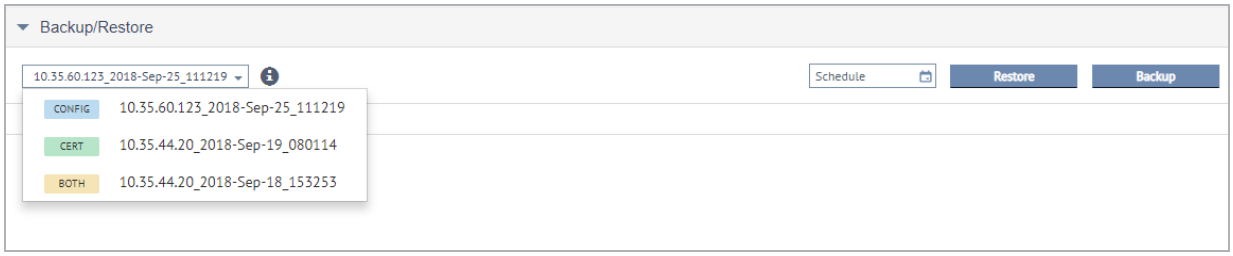


2. Select a network (as shown in the first image), to backup multiple units. To back up a single unit, navigate to that unit in the network tree (as shown in the second image)t

3. Select the **System Configuration** tab.

4. Expand the **Backup/Restore** section.

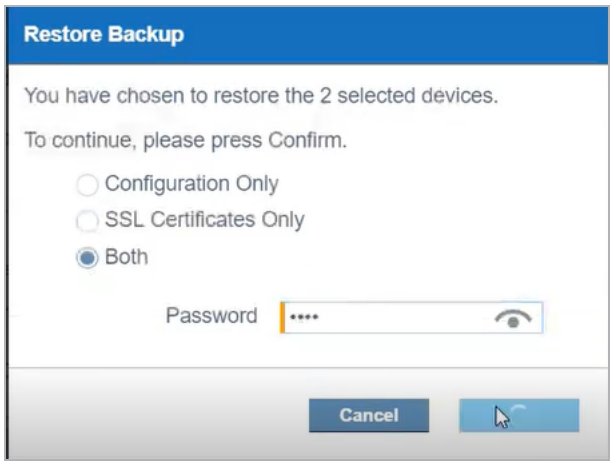
5. If you selected a network, select the LoadMasters that you would like to back up. If you selected a single LoadMaster, select that LoadMaster. You can select the **Select All** check box to select all LoadMasters.



A pop-up message appears with three options:

- **Configuration Only**: Select this option to back up your LoadMaster configuration only.
- **SSL Certificates Only**: Select this option to back up your SSL certificates only.
- **Both**: Select this option to back up both your LoadMaster configuration and SSL certificates.

6. Click the **Select a backup to restore** button and select the desired backup file.



7. A dialog box appears showing you what files are contained in that backup.
8. Type your password that you used to create the backup.
9. Click the **Restore** button.
10. A message appears when the restore completes.

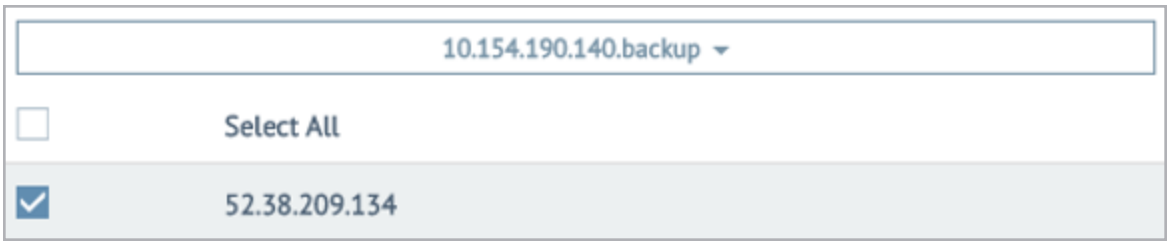
Note that you cannot schedule a restore.

LoadMaster backup archives are not included in Kemp 360 Central backup archives. If you want to create copies of your LoadMaster backups, download them manually to another device.

8.5.4 Schedule a LoadMaster Backup

By carrying out the following steps, users can schedule the backup of a single or multiple LoadMasters, in the future:

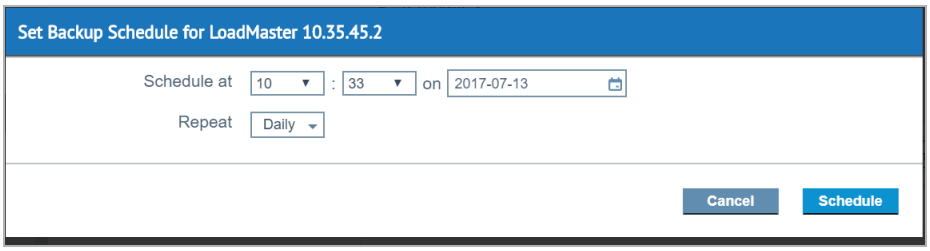
1. Click the cloud icon on the left of the screen.
2. Select the **System Configuration** tab.
3. In the left-hand menu, click the network to which the LoadMaster or LoadMasters you wish to schedule for a backup is attached.



4. Expand the **Backup/Restore** section.

5. Select the check box of the LoadMaster or LoadMasters you wish to backup and click the **Schedule** button.

If you wish to schedule a backup of all LoadMasters in a network, enable the **Select All** check box.



6. Enter the time, date and frequency, for which you wish to schedule the backup.

> Tasks cannot be scheduled within one hour of each other.

7. Click **Schedule**.

8.5.5 Back up and Restore Kemp 360 Central

As a Kemp 360 Central administrator, you can back up your Kemp 360 Central configuration using controls provided within the UI. This includes data related to the following features:

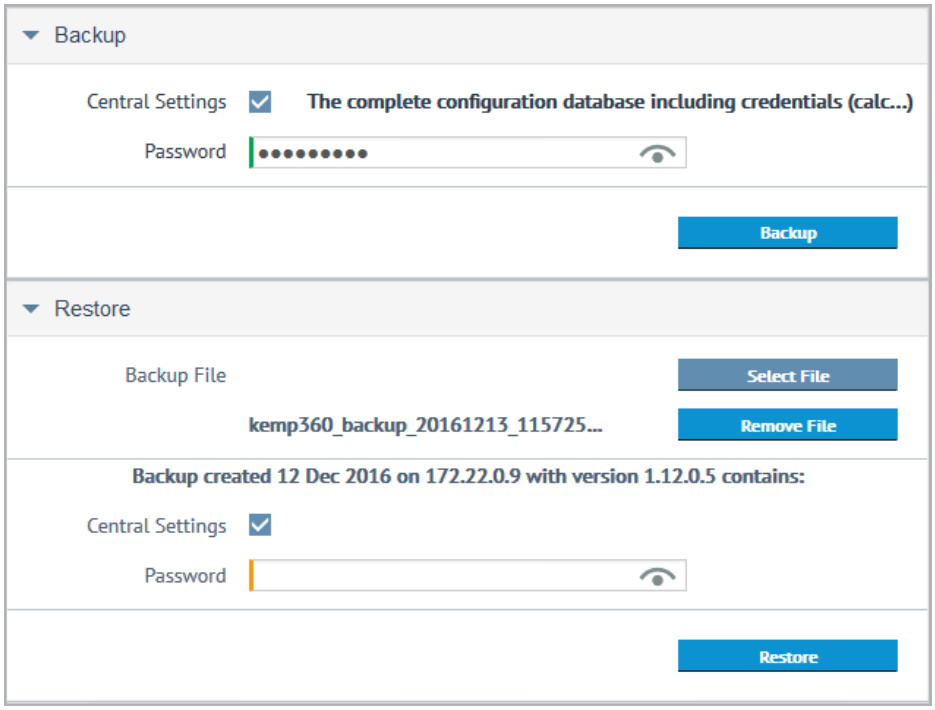
- **Configuration Management** (for example, application profiles and server pools)
- **Reporting** (for example, daily Metered Licensing usage reports)
- **Scheduled Actions** (for example, reboots and backups)
- **Storage** (retention policies)
- **UI Access Control** (for example, server certificates and whitelists)
- **Network Settings** (DNS configuration)

- **Template Management** and **Backup Repository** are included from the **Global Repository**
- Kemp 360 Central settings (for example, SMTP and public keys)

> Note that log data and LoadMaster software updates from the **Global Repository** are not included.

To use the Backup feature, follow the steps below:

1. Click the **Settings and Configuration** icon.
2. Click **Backup & Restore**.

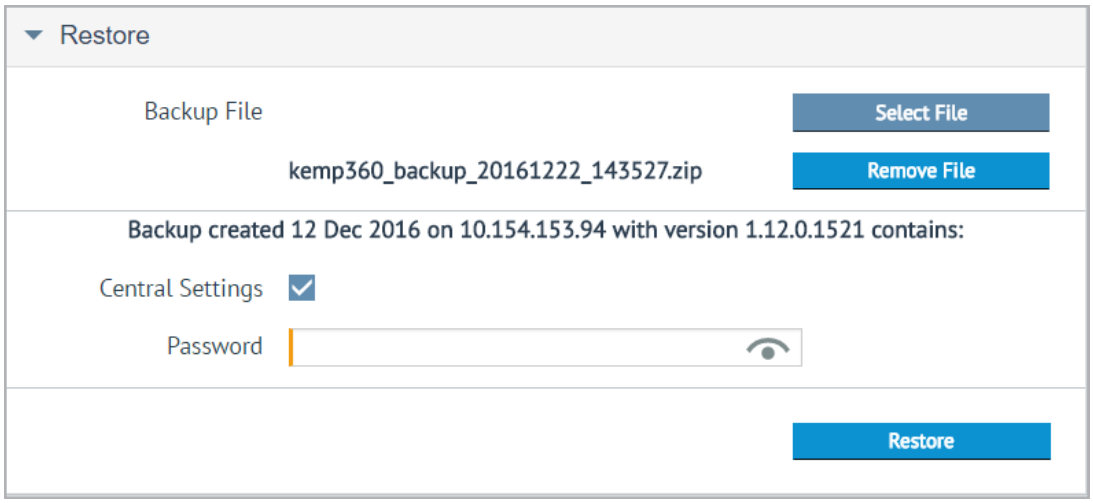


3. Type a password then click **Backup**. For details on password requirements, see the **Appendix: Password Information**. Depending on your browser, this prompts you to download a backup file in your **Downloads** folder or in a location you select.
4. Save the backup to the location where you want to store it.

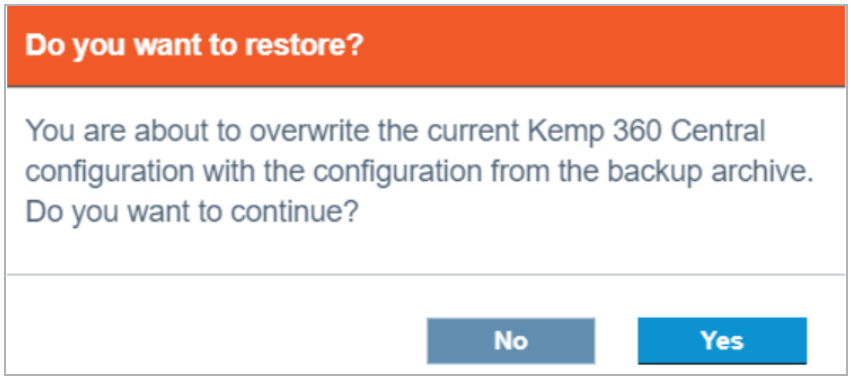
To restore the backup file, follow the steps below:

1. Click **Select File** and browse to the location where the backup is stored.
2. Select the file then click **Upload & Check**. You can view the progress of the upload in the progress bar. If the upload is successful, you will see a notification on the screen.

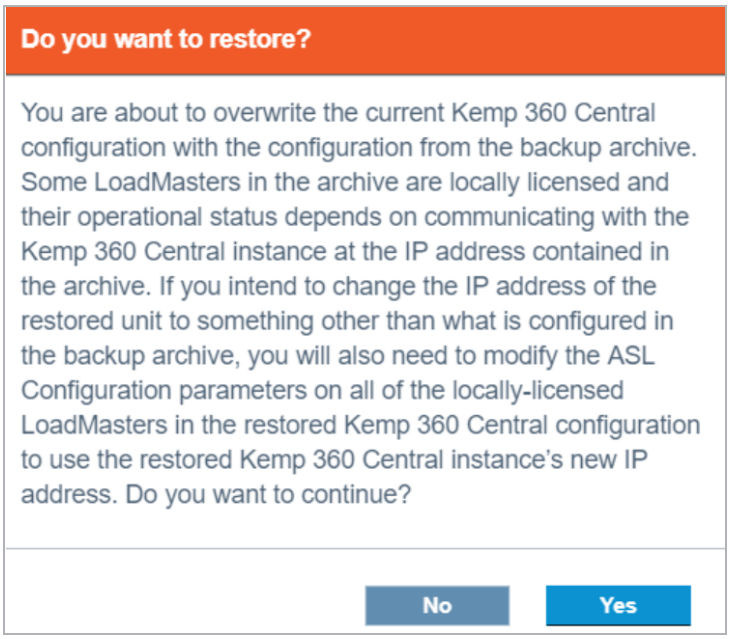
The Kemp 360 Central instance on which you are restoring the archive must be licensed outside of the backup process and the license applied must match the license in effect on the system where the backup archive was created. If the license information does not match, the restore process will not continue.

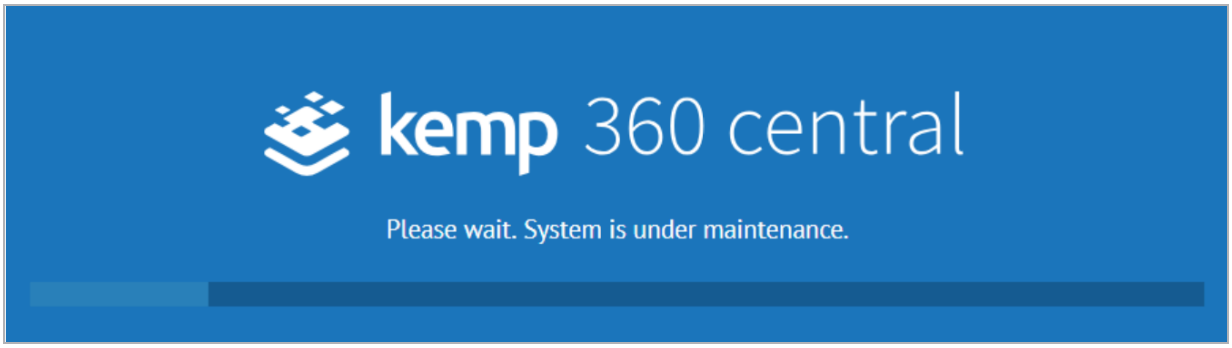


3. Type the password used to create the backup archive, then click **Restore**.



4. Click **Yes** to the message that appears. For locally licensed LoadMasters, the following screen appears while the backup is being restored:





While a restore operation is in progress, API and UI access to Kemp 360 Central is blocked.

5. After the operation completes, log in again.

8.5.6 Configuring Syslog Collection from Managed Devices

You can configure Kemp 360 Central to collects logs from all managed devices that support exporting logs to a syslog server. This includes: LoadMaster, F5, NGINX, and HA-Proxy ADCs. (AWS ELB does not currently support remote syslog functionality.)

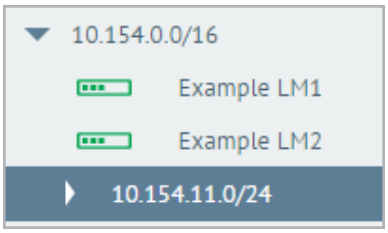
- For LoadMaster, the appropriate syslog options on LoadMaster are configured by Kemp 360 Central when the device is added to Kemp 360 Central and the LoadMaster is contacted for the first time.
- For other devices, you must add the Kemp 360 Central IP address to the list of remote syslog hosts using the UI for that device.

8.5.7 LoadMaster Syslog Collection

When a LoadMaster is first added to Kemp 360 Central, the Kemp 360 Central IP address is automatically appended to the existing list of syslog hosts. After this is set, all logs are sent to Kemp 360 Central and can be downloaded using the Kemp 360 Central interface. For more information relating to downloading the logs, refer to the **System Logs** section.

For a LoadMaster connected to Kemp 360 Central, you can edit the LoadMaster syslog settings using Kemp 360 Central by performing the following steps:

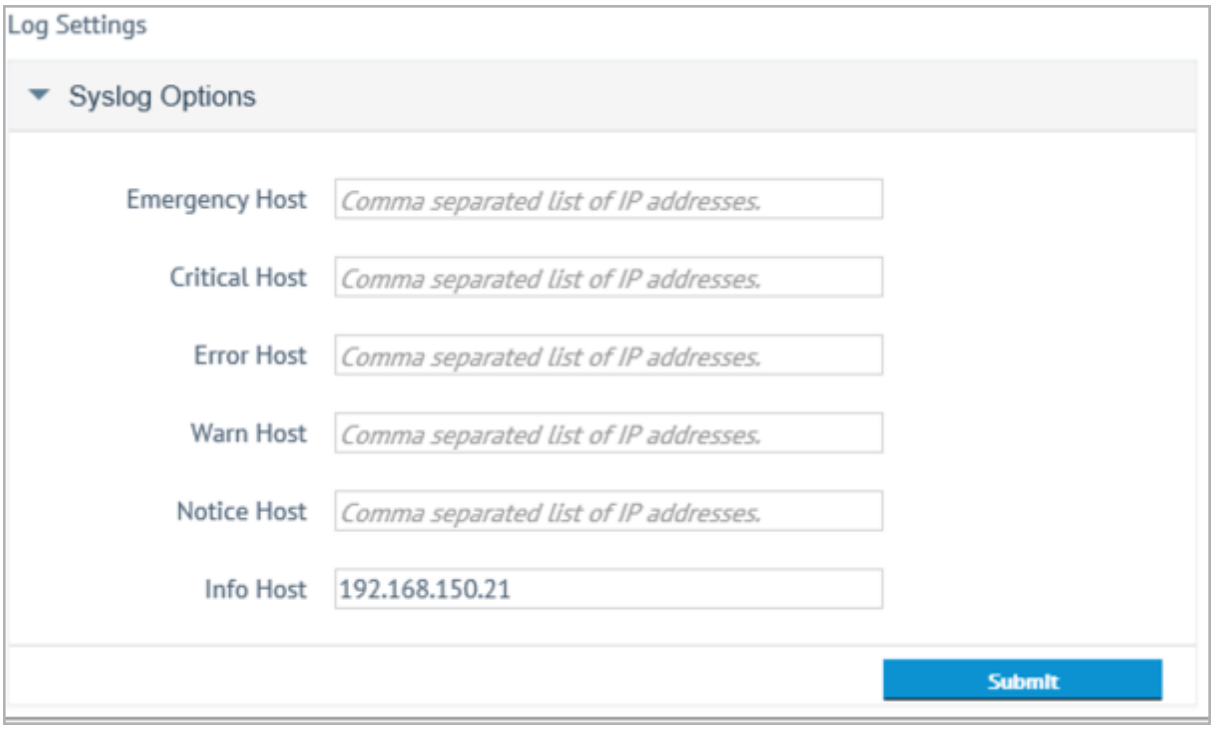
1. Click the cloud icon on the left of the screen.
2. Select the **System Configuration** tab.



3. Select the LoadMaster with the settings you wish to update.

> When updating the syslog targets for a LoadMaster HA pair, use the shared IP address.

4. Go to **Log Settings**.
5. Expand the **Syslog Options** section.



6. Enter the relevant IP addresses of the one or more remote syslog servers in the relevant text boxes. Multiple IP addresses must be separated with a comma.

> You are only able to configure one IP address to one host level. If you try to configure the same IP address that is already set to a syslog host, the IP address host is updated to the new one and you must set a new IP address for the original level. For example, you have the IP address 10.35.60.166 set on the **Error Host** field. If you type the same IP address in the **Critical Host** field, when you click **Submit**, the **Critical Host** is updated with the new IP address but the **Error Host** field will now be blank. You will receive a notification to indicate that the change was successful.

7. Click **Submit** to save the changes.

The syslog settings are then updated on the selected LoadMaster(s). The Kemp 360 Central view of the LoadMaster Syslog Options always remains correct.

Six different error message levels are defined and each message level may be sent to a different server. Notice messages are sent for information only; Emergency messages normally require immediate user action.

Up to 10 individual IP addresses can be specified for each of the Syslog fields. Multiple IP addresses must be separated by commas.

The following are examples of the type of message that may be seen after setting up a syslog server:

- **Emergency:** Kernel-critical error messages
- **Critical:** Unit 1 has failed and unit 2 is taking over as master (in a High Availability (HA) setup)
- **Error:** Authentication failure for root from 192.168.1.1
- **Warn:** Interface is up/down
- **Notice:** Time has been synced
- **Info:** Local advertised Ethernet address

Syslog messages cascade in an upwards direction. Thus, if a host is set to receive WARN messages, the message file will include message from all levels including and above WARN but none for levels below.

If all six levels are set to the same hostn - multiple messages for the same error are sent to the same host.

8.5.7.1 Syslog Collection for F5, NGINX, and HAProxy

For F5, NGINX, and HAProxy devices, syslog collection must be enabled manually on the device through the native user interface. Once the device has been added to Kemp 360 Central and Kemp 360 Central is added as a syslog target to the device, Kemp 360 Central automatically starts collecting logs from these devices.

See the documentation for the device to configure remote syslog options to include the Kemp 360 Central IP address. Documentation current at the time this document was last updated is available at these links:

- **F5**: https://support.f5.com/kb/en-us/solutions/public/13000/000/sol13080.html
- **NGINX**: http://nginx.org/en/docs/syslog.html
- **HAProxy**: http://cbonte.github.io/haproxy-dconv/1.6/configuration.html#log
  http://cbonte.github.io/haproxy-dconv/1.6/configuration.html#8

8.6 Licenses

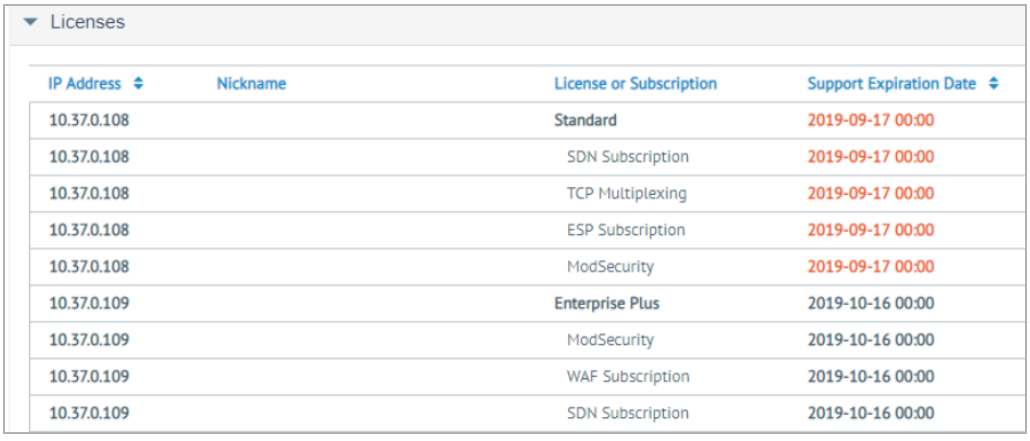
A summary of license details for all the LoadMasters in All Networks or a specific network can be displayed by clicking **Network and Device Administration**, selecting the appropriate network node in the network hierarchy, clicking **System Configuration**, and opening the **Licenses** section. You can display the Licenses section for all networks by clicking **Network and Device Administration > System Configuration**. You can also display the License section for all networks by clicking the **Global Dashboard** icon then clicking **View List** on the **Support Subscription Expiry** widget.

By default, the licenses are sorted by IP address in ascending order. You can change the order of displayed results by clicking the arrows next to the **IP Address** column and the **Expiration Date** column. In the **License or Subscription** column the license type is displayed first and any subscription-based licenses will be indented below this.

> A Classic license refers to a non-subscription-based (or legacy) license.

If you add a LoadMaster, it should appear in the Licenses table without having to refresh the page. If you do not see it, you may need to check the credentials specified for the device on Kemp 360 Central. Similarly, if you delete a LoadMaster, it will be removed from the list. Any LoadMasters that have passed their expiration date will appear in red in the **Expiration Date** column.

> The **Licenses** table does not list any devices that are down or otherwise unreachable.



> For LoadMaster HA Pairs, there is no licensing information displayed for the HA Shared IP Address ‘device’. This is

because the HA Shared IP does not belong to one particular device, but instead is passed between the two HA units. To see the licensing information for a LoadMaster HA Pair, you must look at the licensing information for the individual HA units in the pair.

8.7 HA Configuration

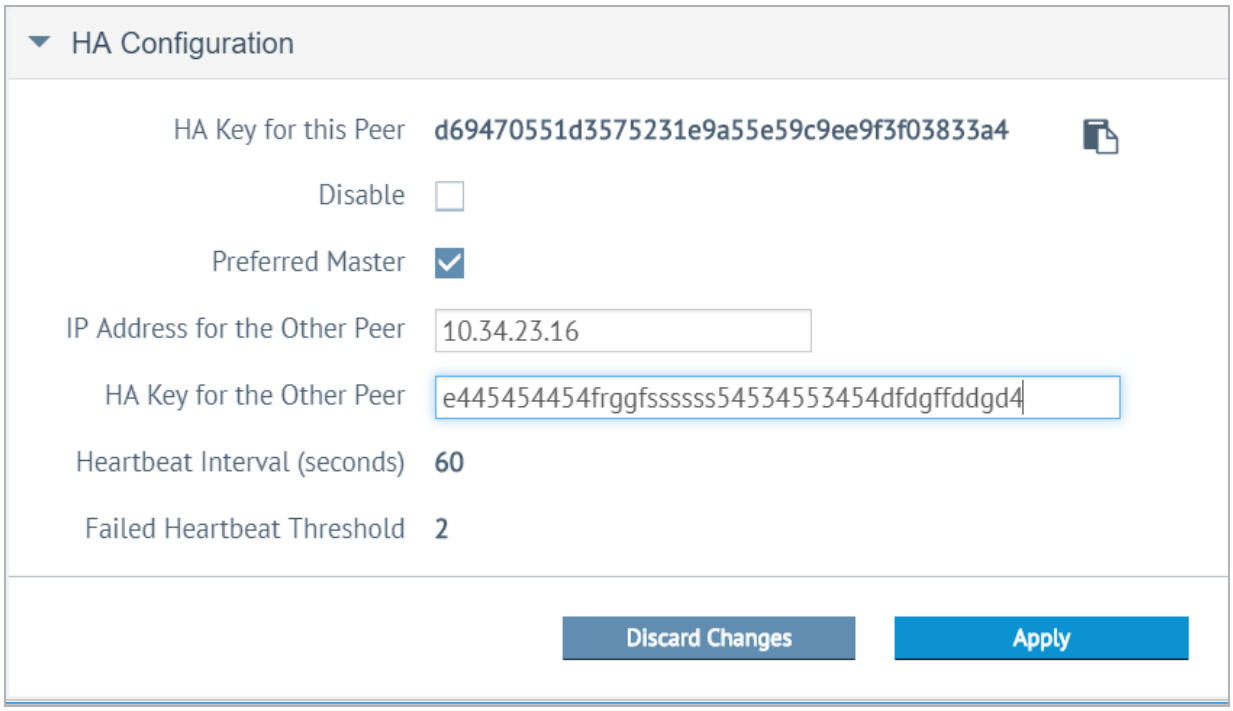
In the **HA Configuration** section (**Settings and Configuration > HA Configuration**), you can configure two Kemp 360 Central instances into a master-slave High Availability (HA) configuration as follows:

- Both HA units are active in terms of enabling you to make changes to Kemp 360 Central and managed device configuration, synchronization of data, and gathering syslog output from managed devices.
- Only the master unit generates statistics and communicates these to the slave unit periodically.
- Scheduled actions can be configured on either unit and are communicated to the other unit, but they are executed only by the current master unit.

Under normal operating conditions the master processes the scheduled tasks and the slave synchronizes repository files from the master. If the slave fails, nothing happens, but when it recovers, it checks if the master is up. If the master is not up, the slave becomes the master. If the master is up, the slave synchronizes repository files from the master.

When configuring two Kemp 360 Central instances into HA mode, both units must have at least one network defined for the initial synchronization to complete successfully. When the initial synchronization is complete, changes are propagated in both directions.

Before configuring two Kemp 360 Central instances into HA mode, decide which unit you want to be the Preferred Master. The Preferred Master always assumes the master role in the HA configuration when it is available. The other unit becomes the Preferred Slave; should the Preferred Master become unavailable, the Preferred Slave takes over from the master and returns control to the Preferred Master once it is available again.



> LoadMaster profiles and target environments are not currently synchronized between Kemp 360 Central HA units.

To configure two Kemp 360 Central instances into HA mode, perform the following steps:

> If the Kemp 360 Central units that you are configuring into an HA pair already have configurations on them, determine which of the configurations you want to keep (if any). The system that has the configuration you want to keep should be configured first, so that it goes into **Master** mode. The configuration on the other unit will be overwritten when it assumes the **Slave** mode.

1. Open the Kemp 360 Central UI of both units that you want to configure into HA mode (**Settings and Configuration > HA Configuration**).

2. On the UI of the unit that you want to make the **Slave**, copy the **HA Key for this Peer** from the **HA Configuration** section.

3. On the UI of the unit you want to become the **Master**:

a) Paste the HA Key you copied in the previous step into the **HA Key for the Other Peer** field.

b) Select the **Preferred Master** check box.

c) Type the IP address of the **Slave** unit into the **IP Address for the Other Peer** field.

d) Click **Apply**.

> Wait until the **Our State** field in the **HA Status** section indicates that this unit has assumed the **Master** state before moving on to the next step. This is critical to ensuring that both units assume the desired state and the intended configuration is propagated. This may take a few minutes.

4. On the UI of the unit that has just entered the Master state, copy the **HA Key for this Peer** from the **HA Configuration** section.

5. On the UI of the unit you want to become the **Slave**:

a) Paste the **HA Key** you copied in the previous step into the **HA Key for the Other Peer** field.

b) Type the **IP address** of the **Slave** unit into the **IP Address for the Other Peer** field.

c) Click **Apply**.

> Wait until the **Our State** field in the **HA Status** accordion indicates that this unit has assumed the **Slave** state. This may take a few minutes.

The HA Configuration is complete once the HA status accordion shows that one unit is in the Master state, one unit is in the Slave state, and that heartbeats are being actively exchanged between the two HA units.

> Both Kemp 360 Central HA units try to contact one another every 30 seconds; this is called a heartbeat and is the method by which the two units determine when a fail over should occur. Since these heartbeats occur every 30 seconds, there can be up to a 30-second delay between the time that the current master HA unit becomes unavailable and the time that

the current slave becomes aware of the outage and attempts to take over the master role.

The sequence number is mainly used for debugging and should match the sequence number on the peer. This is useful to check if the pairs are working correctly.

If the master goes down, this can be viewed in the HA Status panel after 30 seconds. If you click **Refresh**, you see the error and the number of heartbeats that were missed. The slave now becomes the master. Once the original master comes back online, the system reverts to the original master if you selected the **Preferred Master** check box when you configured it.

You can configure a LoadMaster HA pair within a Kemp 360 Central HA pair.

8.8 HA Configuration in Kemp 360 Central Metered Licensing Deployments

When you have a Kemp 360 Central HA pair deployed in a Metered Licensing environment, both units must be running the same version of Kemp 360 Central. If you upgrade one unit in the pair, you must upgrade the other unit as soon as possible to maintain consistent HA operation.

For Metered Licensing HA, Kemp 360 Central checks that the following are true at every HA poll:

- Both units have the same local license setting – that is, they are either both licensed for local licensing or are both not licensed for local licensing.
- Both units have the same Metered Licensing license setting – that is, they are either both licensed for Metered Licensing or are both not licensed for Metered Licensing.
- Both units are running the same version of Kemp 360 Central.

If any of these values are not true, Kemp 360 Central returns an error and moves itself into standalone mode (that is, out of HA mode).

The most likely reasons for this occurring are: one of the HA units' license was updated or a backup was restored to one or both of the units, which resulted in a licensing mismatch between the units.

Managed LoadMasters can grab a license from either Kemp 360 Central unit and can re-license against either unit; the license then 'migrates' from one Kemp 360 Central unit to the other. Note that if the LoadMaster re-licenses from both units in quick succession, both units may indicate that

the LoadMaster is licensed by the other unit. This can be addressed by re-licensing the unit again, and then waiting a few minutes for the re-license to synchronize across the pairs.

Metered Licensing reports from either HA unit contain all Metered Licensing LoadMasters licensed across both Kemp 360 Central HA units. A unit licensed against the 'other' peer is indicated in the Metered Licensing report by including the device ID from the other Kemp 360 Central HA unit in parentheses:

If one of the Kemp 360 Central HA units in a pair is removed from the HA pair, all actively licensed LoadMasters are moved to the other Kemp 360 Central unit as 'normal' (that is, not activated by Kemp 360 Central) devices. These units must be re-licensed against the remaining Kemp 360 Central unit. To do this, you must:

- Remove the existing normal (green) unit from Kemp 360 Central.
- Re-license the LoadMaster from the LoadMaster web user interface (UI) against the remaining Kemp 360 Central instance.

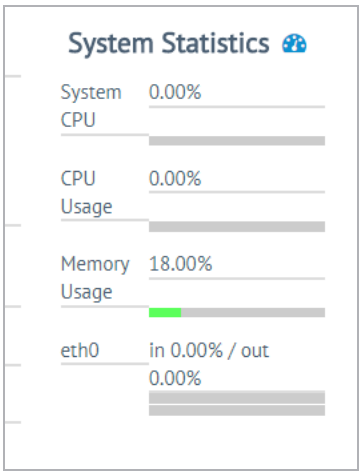
In releases before Version 1.23, it was not possible to take a backup from one HA unit (for example, the Master) and use it to replace the other unit (the Standby) in the HA pair; this broke the HA configuration.

In Version 1.23 and later releases, doing the above no longer breaks the HA configuration, but you must still check that the **Disable**, **Preferred Master**, **IP Address for the Other Peer**, and **HA Key for the Other Peer** settings are correct for your configuration. That is, under normal operation, neither unit should be disabled, only one unit should have the **Preferred Master** option selected, and the **IP Address for the Other Peer** and **HA Key for the Other Peer** should contain information obtained from the UI for the other unit in the HA pair.

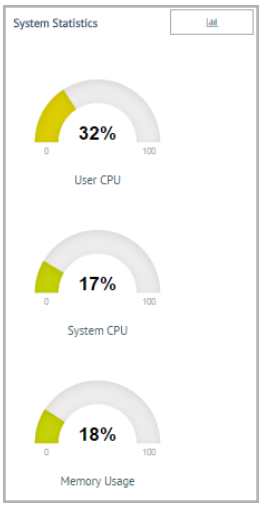
9 Monitoring

The **Monitoring** section of Kemp 360 Central displays the overall health of your HA pairs, Virtual Services, Real Servers, SubVSs, and WAF Statistics (if configured). All statistics update every minute.

> In a LoadMaster HA pair configuration, only the shared IP node has a Monitoring section. HA1 and HA2 units do not have a Monitoring section.



System Statistics are updated every minute. In the list view, as the percentage used increases - the bar changes from empty (at 0%) to green (1%) through white (50%) to dark red (99%).

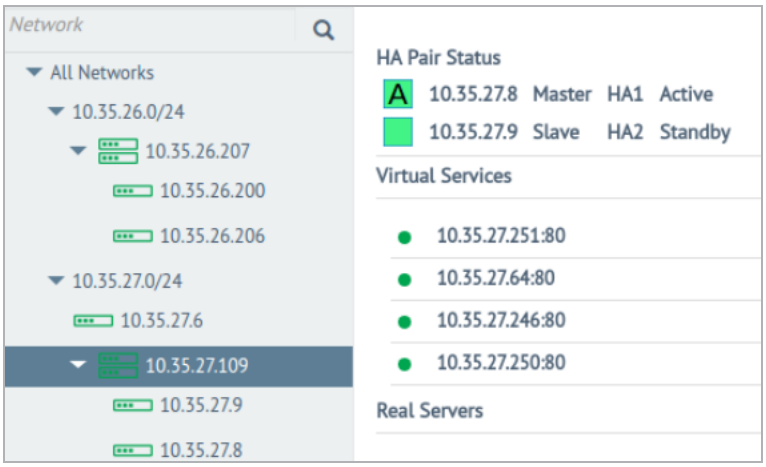


To display the gauges as shown in the figure above, users should click the button with the gauge icon.

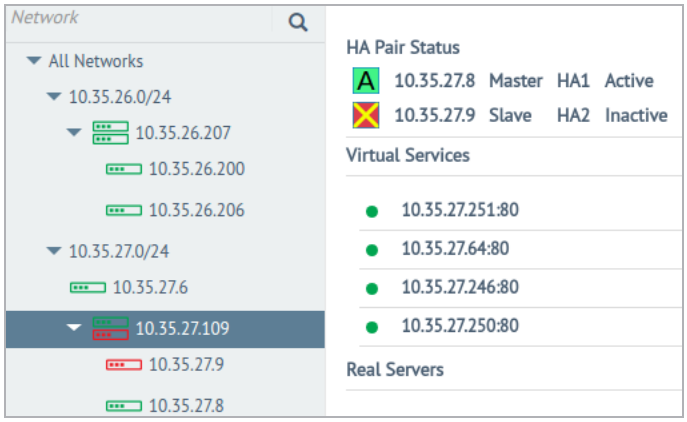
The **System Statistics** section enables users to monitor the following:

- The percentage of the CPU spent processing in user mode
- The percentage of the CPU spent processing in system mode
- The amount of memory in use and the amount of memory free
- The list view shows the percentage traffic that passes through each eth interface
- Using the **System Statistics** section gives users the ability to monitor the statistics for an individual device.

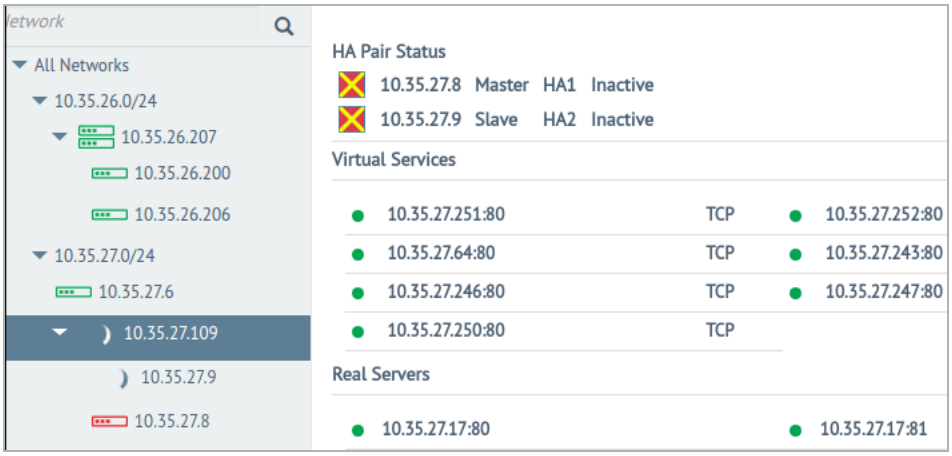
There are a number of different LoadMaster HA statuses that could be present depending on whether units are active, in standby, or inactive as shown below. This status is maintained using an automatic ping between the units.



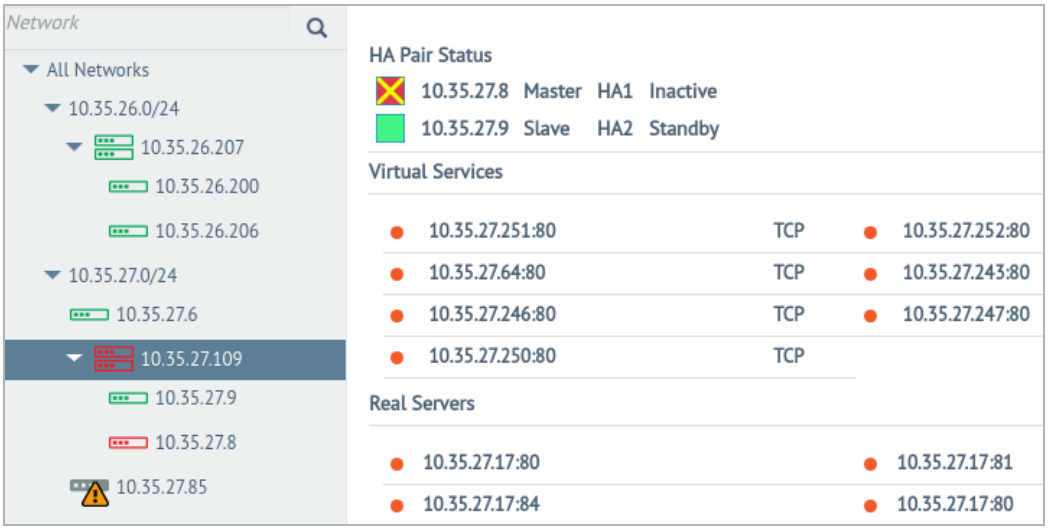
The unit above is online and operational and the HA units are correctly paired. The A in the middle of the square indicates that this is the master (active) unit. The absence of an 'A' in the middle of the square indicates that this is not the master unit (standby).



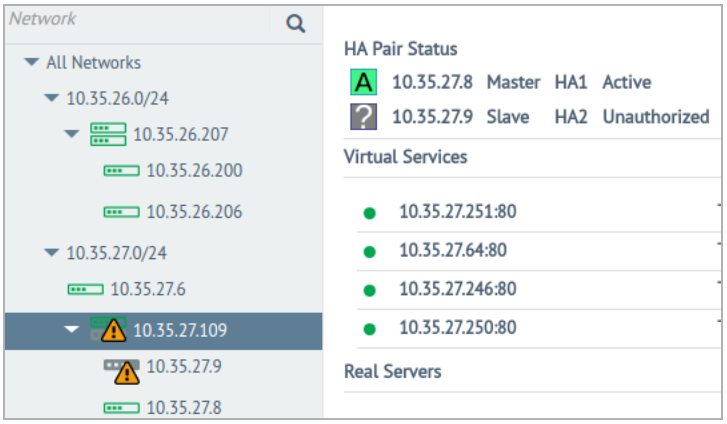
The master unit above is online and operational but the slave may be offline or misconfigured.



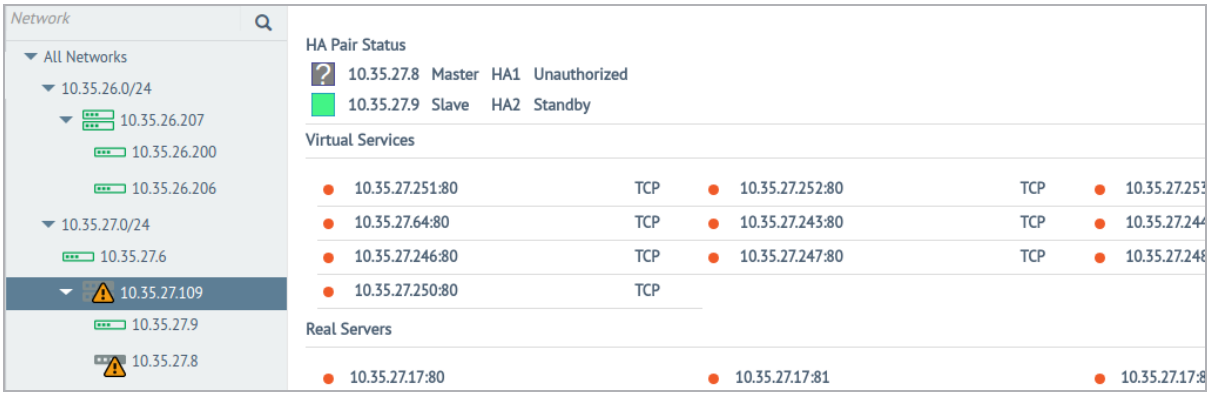
Both the master and slave units above are offline or misconfigured.



The master unit above is offline or misconfigured but the slave is in standby and operational.

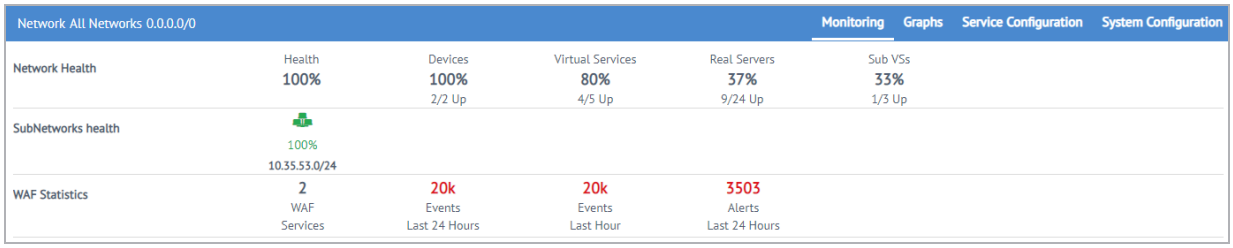


The master unit above is online but the HA status is unknown because the last connection to the device failed. Check the credentials of the device and log (both on the device and on Kemp 360 Central).



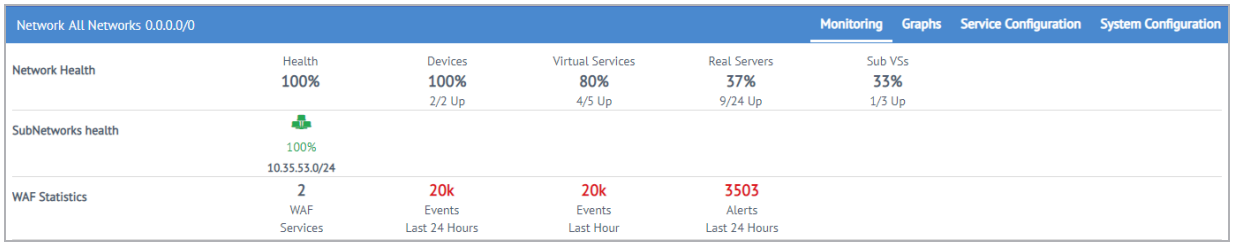
The slave unit above is online but the HA status is unknown because the last connection to the device failed. Check the credentials of the device and log (both on the device and on Kemp 360 Central).

> If you have WAF services configured, you can view WAF details at the network (includes all sub-networks), sub-network (that sub-network only), and individual device level.



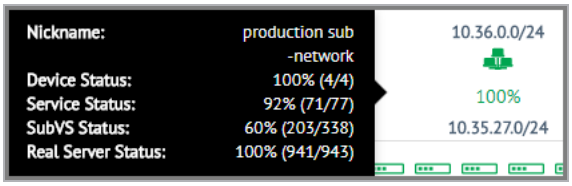
9.1 Network and Device Health

To view the overall network health of all networks in Kemp 360 Central, click **All Networks**. This informs you about the overall health percentage of your network including the number of devices, Virtual Services, Real Servers, and Sub VSs that are up or down.



This section of the document fully explains the various sections and headings shown in the screenshots above. **Network Health** shows an aggregated health percentage value for the network currently selected in the left frame, calculated using the number of devices with an UP status on the network, against the total number of devices in that network. A separate health value is displayed for **Devices**, **Virtual Services**, **Real Servers**, and **SubVSs**.

SubNetworks health shows the status of each subnet individually. The subnetwork health percentage is based on the number of UP devices in the subnetwork against the total number of devices in that subnetwork.

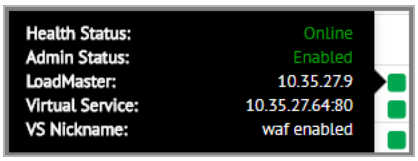


Hovering over the subnetwork health icon displays the **Nickname**, **Device Status**, **Service Status**, **SubVS Status**, and **Real Server Status**.

In the **Devices** section, an icon is displayed for each device on the network. A red icon means that the device is down. A grey icon means the device is disabled. A green or blue icon means the device is up (blue is used to indicate a LoadMaster that was licensed using the local licensing functionality).

Hovering over the device icons displays the device type, IP address, the status of that device, and the device nickname - if available.

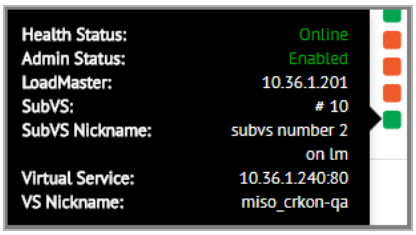
Hovering over the header at the top of the User Interface (UI) also displays the full nickname for the device.



When a network is selected on the left, the **Real Servers** section displays – if available. In the **Real Servers** section, there are icons for each **Real Server** on the network. Green indicates the **Real**

Server is up while red means the **Real Server** is down. Hover help displays the **Health Status**, **Admin Status**, **LoadMaster** IP address, **Virtual Service** IP address, and the **VS Nickname**, if available, of individual **Real Servers**.

When a network is selected on the left, the **Real Servers** section displays – if available. In the **Real Servers** section, there are icons for each Real Server on the network. Green indicates the Real Server is up while red means the Real Server is down. Hover help displays the **Health Status**, **Admin Status**, **Loadmaster** IP address, **Real Server** IP address, **Virtual Service** IP address, and the **VS Nickname**, if available, of individual Real Servers.



In the **SubVSs** section, there are icons for each SubVS on the network. Green indicates the SubVS is up while red means the SubVS is down. Hover help displays the **Health Status**, **Admin Status**, **Loadmaster** IP address, **SubVS** number, **SubVS Nickname**, if available, **Virtual Service** IP address, and the **VS Nickname**, if available, of individual SubVSs. The **SubVS Nickname** displayed on Kemp 360 Central is the same as the nickname used for that SubVS on the LoadMaster. The tooltip displays the full **SubVS Nickname**. The SubVS number is the same number used on LoadMaster on the SubVS configuration screens (click **View / Modify Services > Modify > SubVSs**); they are not the numbers displayed in the **View /Modify Services** table).

When users select an individual LoadMaster, the status of its Virtual Service(s) and Real Server(s) appears above the **Connections** graph, as shown in the following figure:

A green icon indicates that the Virtual Service or Real Server is up, a red icon indicates it is down and a grey icon indicates it is disabled.

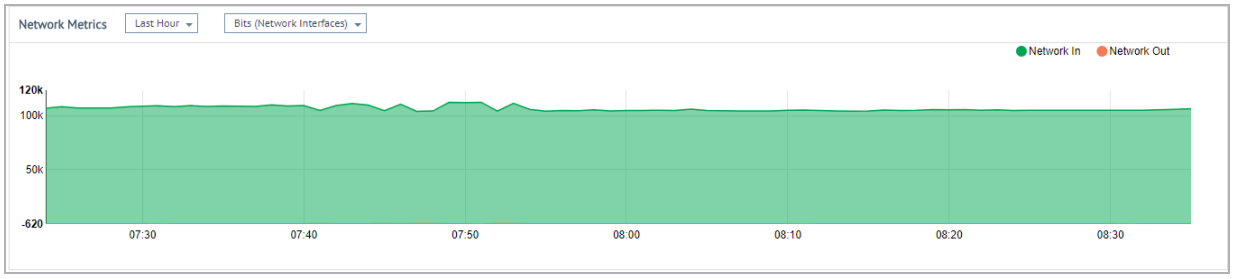
> The shared IP is not found in **Network and Device Health**.

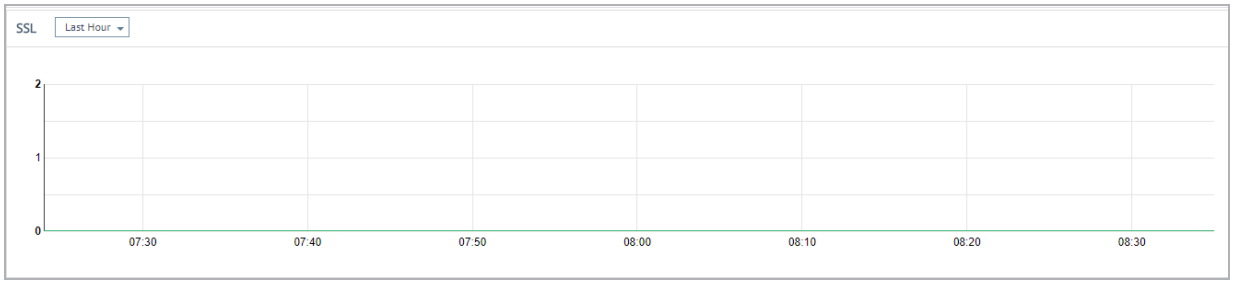
9.2 Graphs

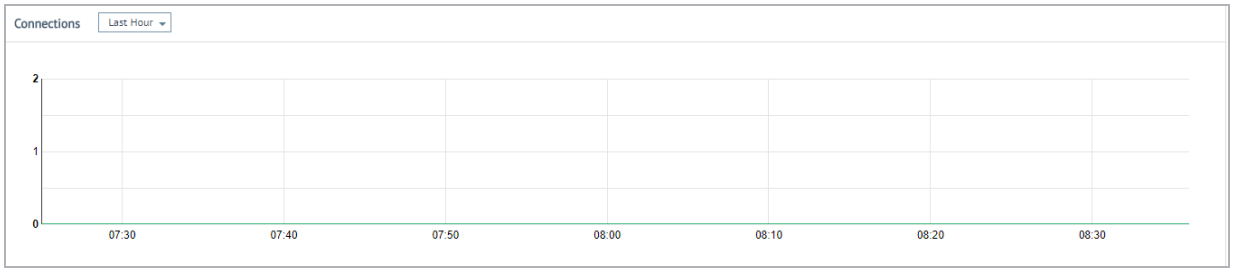
You can view all details relating to Network Metrics in the **Graphs** tab. To view the monitoring section of an individual Kemp 360 Central device, first click on the relevant network or device and then click **Graphs** in the top-right of the screen.

> In a LoadMaster HA pair configuration, only the shared IP has a graph.

By clicking the drop-down arrow, you can display data ranging from the past hour to several years ago. In addition, all three graphs use the same horizontal width/scale so that time-based comparisons between the graph data are easier to visualize.







The **Network Metrics** graph displays activity in and out of the Network Interfaces. You can display results in Bits (Network Interfaces), Bytes (Network Interfaces) or Packets (for Virtual Services) per second. You can also view results using various time scales from the last hour to the last 2 years. The graph is broken down into 72 data points so whatever timeframe you select is divided by 72. For example, if you select 1 year, then each data point is approximately 5 days. You can also place your cursor at any point on the graph to find the metrics at that time.

The **SSL TPS** graph displays the SSL Transactions Per Second (TPS) for a selected network, subnetwork or LoadMaster. You can display results in a similar way to the Network Metrics graph.

The **Connections** graph displays the total number of connections made to devices in a network or subnet being monitored by the Kemp 360 Central instance. You can display results in a similar way to the Network Metrics graph.

By selecting the appropriate network, subnetwork or LoadMaster icon in the left side-bar, Kemp 360 Central gives users the ability to monitor activity across the entire network (the results shown are an aggregate of the activity for all devices in the network), a subnet (an aggregate of all the devices in the subnet) or for an individual device.

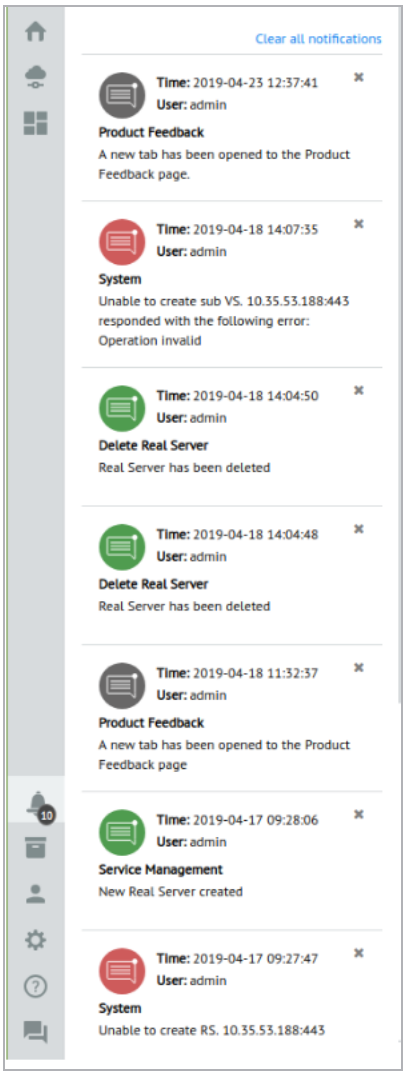
Note that whichever device or network is highlighted in the left side-bar is the device or network you are working with. Please ensure you select the correct one.

10 Notification History

Notifications appear on Kemp 360 Central when specific events occur such as warnings or errors. These are typically messages displayed in small popup windows that appear at the upper right corner of the UI after you execute some operation in the UI (for example, adding a new device), but may also appear due to asynchronous events (for example, a server going down), or scheduled actions (for example, the scheduled backup of a device).

As an **admin** user, you can now view all notifications that appeared on the UI over the past 7 days.

To view the current list of notifications, click the **Notifications** icon on the UI, shown at the top of the above screenshot. The newest notifications appear at the top.



The notifications appear in the same color they originally appeared on the UI:

- Green: Success
- Red: Error
- Grey: Information
- Yellow: Warning

You can view up to 25 notifications at one time. To mark a single notification as read, click the x in the top right. Notifications last for 7 days, after which they are deleted by the system. To clear all notifications, click **Clear all notifications**. To close the **Notifications** window, click anywhere else on the screen.

11 Global Repository

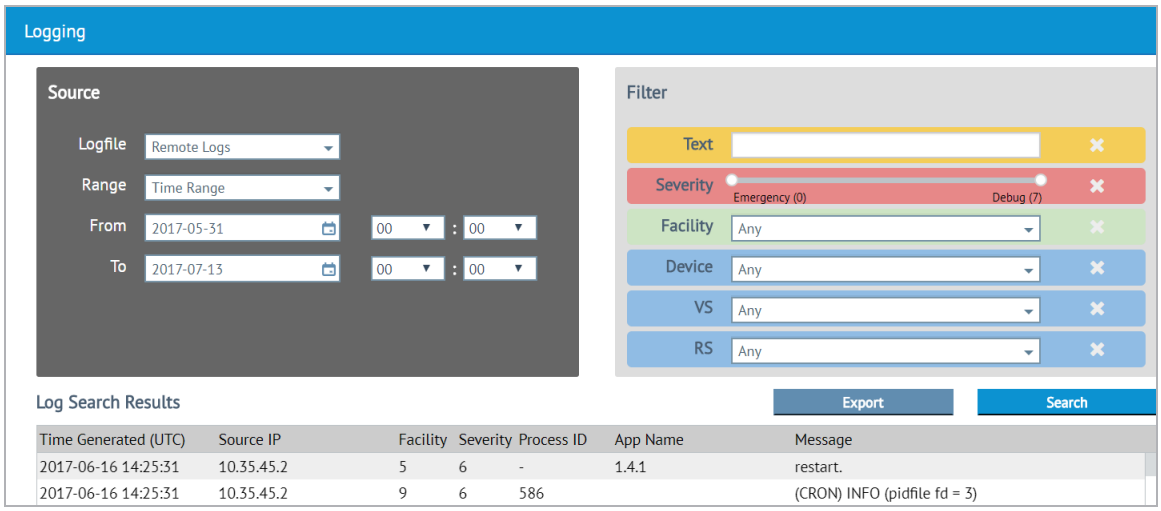
Most of the screens in the **Global Repository** section in the UI relate to uploading files (such as firmware, template and backup files) to Kemp 360 Central. You can then upload these files to LoadMasters using Kemp 360 Central. The **System Configuration** section of this document has details about those features.

To access the **Global Repository** - click the icon in the bottom-left corner of the UI.

11.1 Logging

The **Logging** screen enables you to display the system logs collected from the LoadMasters monitored by Kemp 360 Central. It also enables you to search and filter logs using several different criteria.

> You cannot search for shared IP addresses on the **Logging** page.

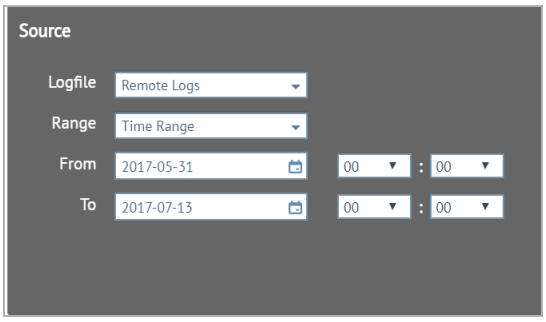


There are three main sections:

- Source
- Filter
- Log Search Results

11.1.1 Source

The **Source** section is located on the top left of the **Logging** screen.



There are two dropdown lists on the **Source** screen, **Logfile** and **Range**.

Logfile: Select the log source you want to display in the **Logfile** drop-down list. Currently, the only selection available is **Remote Logs**.

Range: Select from the following choices to set the time range for the log search:

- Last 24 hours: Searches all log entries with a timestamp that occurred during the 24 hours before the current system time.

- Last Week: Searches all log entries with a timestamp that occurred during
- the 7 days before the current system date.
- Last Month: Searches all log entries with a timestamp that occurred during
- the month before the current system date.
- Last Year: Searches all log entries with a timestamp that occurred during
- the year before the current system date.
- Everything: Searches all log entries.
- Start Time: Searches all log entries with a timestamp that occurred during the time period starting from a user-specific date/time to the current system time.
- Time Range: Searches all log entries with a timestamp that occurred during a user-specified date/time range.

For example, to view logs from midnight January 5th to midnight February 9th 2016:

1. Select **Time Range** from the **Range** drop-down list.
2. Select the required date and time from the **From** field.
3. Select the required date and time from the **To** field.
4. Input any extra filter options then click **Search**.
5. Use the scrollbar to scroll through the results.

11.1.2 Filter

In the **Filter** section, you can further refine your search using several different fields. These are Text, Severity, Facility, Devices, Virtual Server (VS) and Real Server (RS). You can search using just one filter or multiple. The relationship between the fields is an implicit AND. For example, if you specify a device IP and a Real Server IP, only entries that contain both are selected for display. In addition, when you select one of these filters, you are presented with a list of the devices, Real Servers and Virtual Servers that Kemp 360 Central knows about.

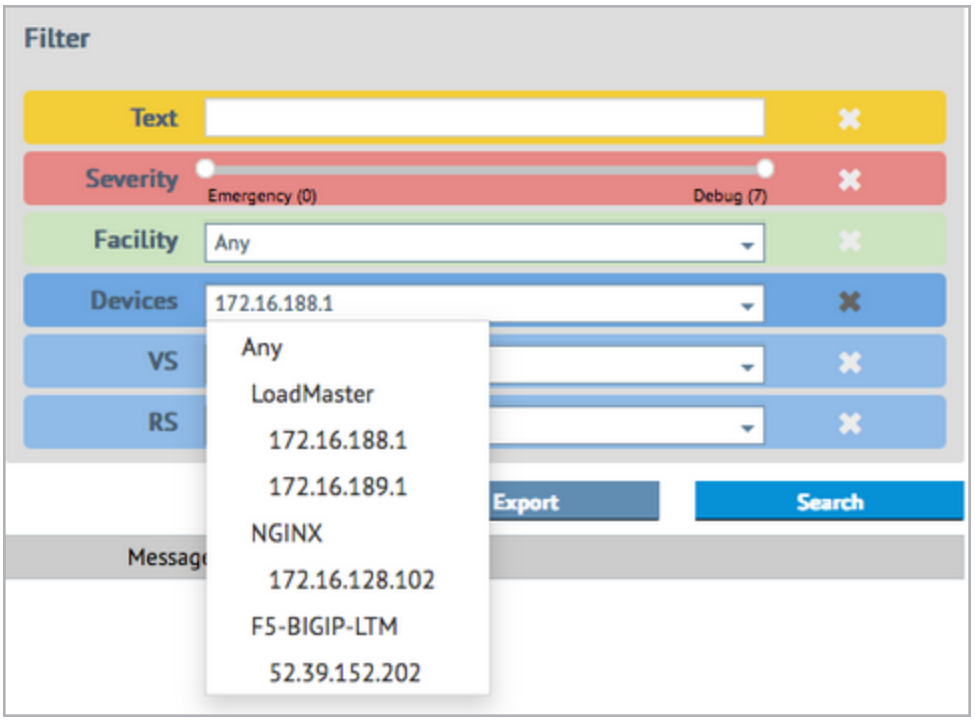
- **Text**: Type a plain text string in the **Text** field to filter the results further. This is a simple text search. Typing any text string selects all log entries that contain that text string anywhere in the entry. For example, if you type an IP address, the log viewer displays all lines that contain that IP address, regardless of what kind of device is

assigned that IP address (LoadMaster, Virtual Service, Real Server, and so on).

- **Severity**: There are a number of levels of severity you can use in your search to filter the log search results. These are shown in the table below:

Value	Severity	Description	Example
0	Emergency	System is unusable	Kernel-critical error messages
1	Alert	Should be corrected immediately	Loss of the primary ISP connection
2	Critical	Critical conditions	One unit has failed and the second unit is taking over as master (in a High Availability (HA) setup)
3	Error	Error conditions	Authentication failure for root from 192.168.1.1
4	Warning	May indicate that an error will occur if action is not taken	Interface is up/down
5	Notice	Events that are unusual, but not error conditions	Time has been synced
6	Informational	Normal operational messages that require no action	An application has started, paused or ended successfully.
7	Debug	Information useful to developers for debugging the application	

- **Facility**: The Facility filter enables you to select the type of log issue you want to search for. For example, kernel messages, user-level messages, mail systems, system daemons, and so on. To select a facility, click the drop-down arrow.
- **Devices, VS, RS**: You can also filter results on specific devices, Virtual Services and Real Servers. The list is arranged by device type, that is, all LoadMasters, all F5 devices, all NGINX devices, and so on, are listed as a group. If you select a device type for the search (for example, click LoadMaster), then all logs for all LoadMasters are searched. If you pick a specific device, then only logs for that device are searched.



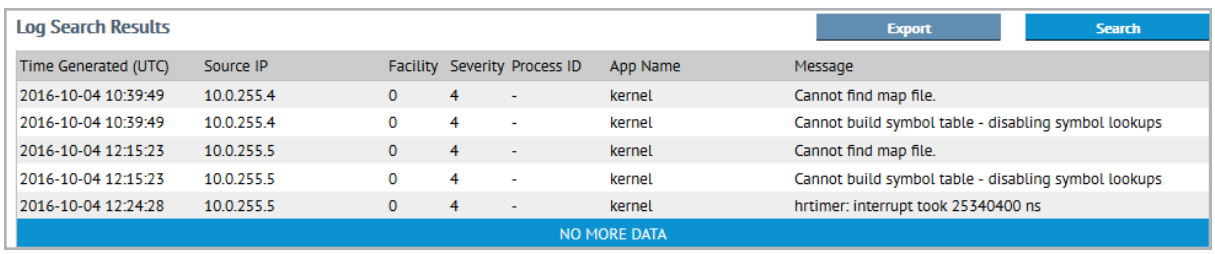
Any field that you use in a search is highlighted. To exclude a filter in a search, click the X on the right of the field. In addition, logging is user-specific. If you log out and log back in again, any data that you used in your search will still be visible, however, it will not be visible to other users.

1. Click **Search** to filter the results based on the specified criteria.
2. Click **Export** to export the results of the filter to a text file.

> To export all log data, select **Everything** from the **Range,** clear any filters that have been set by clicking the X next to them, click **Search**, and then click **Export**.

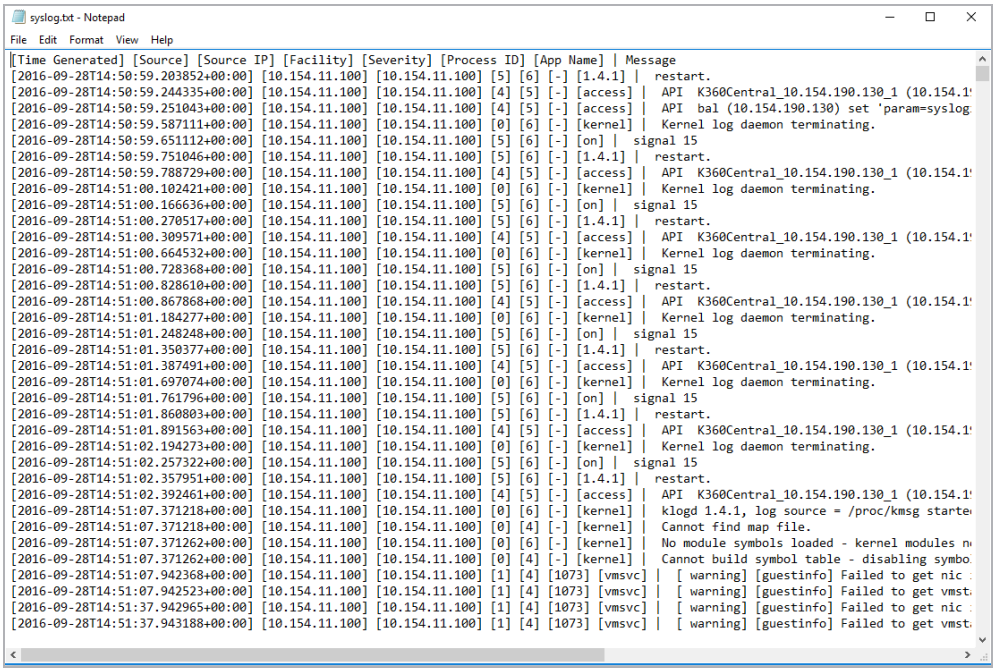
11.1.3 Log Search Results

In the **Log Search Results** section, different columns display the syslog information:



- **Time Generated (UTC):** The generation time of the syslog message.
- **Source IP:** The source IP address of the LoadMaster that the syslog came from.
- **Facility:** The type of program that is logging the message. Messages with different facilities may be handled differently. RFC 3164 defines the list of facilities available.
- **Severity:** The severity of the log file. This is also defined by RFC 3164.
- **Process ID:** The ID number of the relevant process.
- **App Name:** The name of the related application.
- **Message:** The message component has these fields: <tag>, which should be the name of the program or process that generated the message, and <content>, which contains the details of the message.

The figure below displays an example of an exported log file. Note that each field in each line of the log is enclosed within brackets '[ ]' so that the data is clearly delimited.



12 Access Control

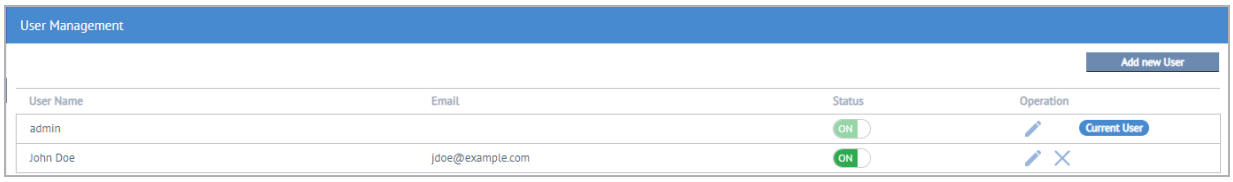
You can administer users in the **User Management** screen, which you access by clicking the **Access Control** icon in the bottom-left of the screen. Here you can manage the different levels of access required by different users.

There is one default user in Kemp 360 Central – the **admin** user. The **admin** user can perform all tasks in Kemp 360 Central. It is not possible to change the permissions of or delete the **admin** user. The **admin** user sets the permissions for new users. There are two permissions, **Read only** and **Write** and these can be set for both **Service Configuration** and **System Configuration**.

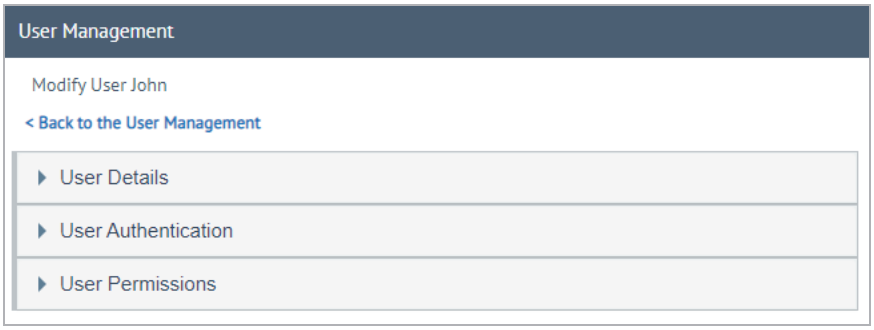
Descriptions of some terminology used in this section are below:

- User: An identity on Kemp 360 Central defined as a username and password.
- Group: A collection of users with assigned permissions to resources.
- Permission: Defines the level of access a user or group has to a resource.
- Resource: A LoadMaster or Virtual Service.

12.1 User Management



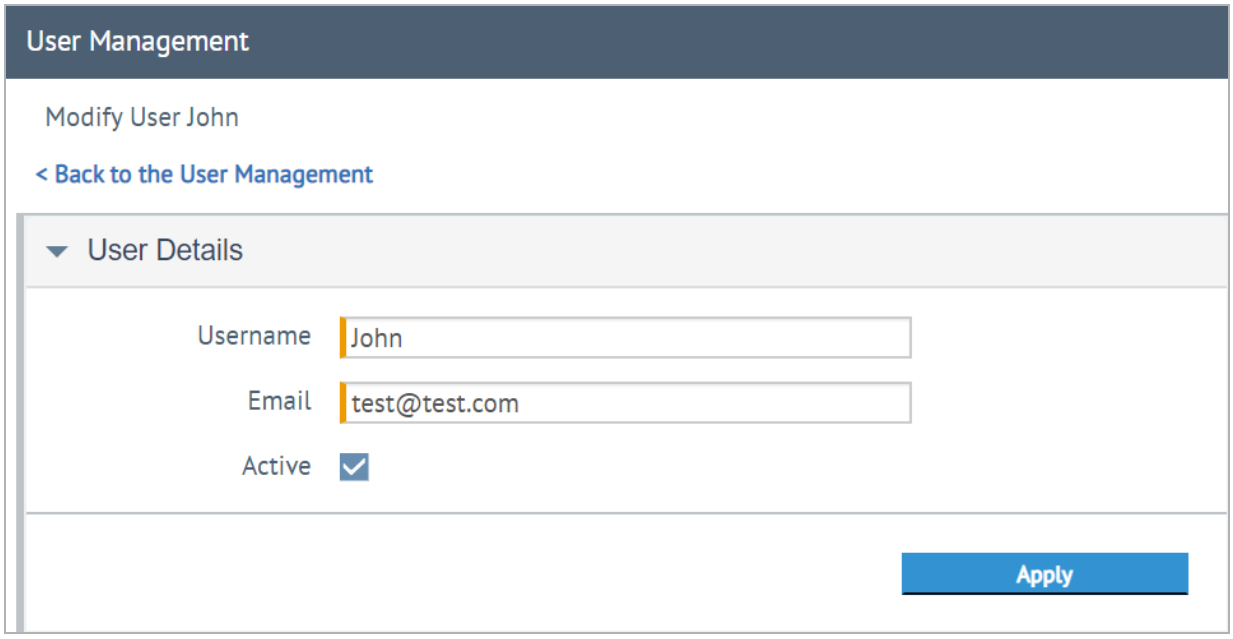
The **User Management** screen lists all Kemp 360 Central users. Here, you can modify, delete, and disable users. You can also add a new user by clicking the **Add new User** button and filling out the details.



To open the **Modify User** screen, click the edit icon of the relevant user. Here, as an **admin**, you can update various details about the user including their password, email address, and permissions. By default, user permissions are set to read only (for details on setting your password, see the **Appendix: Password Information**).

> If you are logged in as a non-admin user, you can update your password, however, you must know your current password. As a non-admin user, you are unable to change user details or user permissions.

User Details



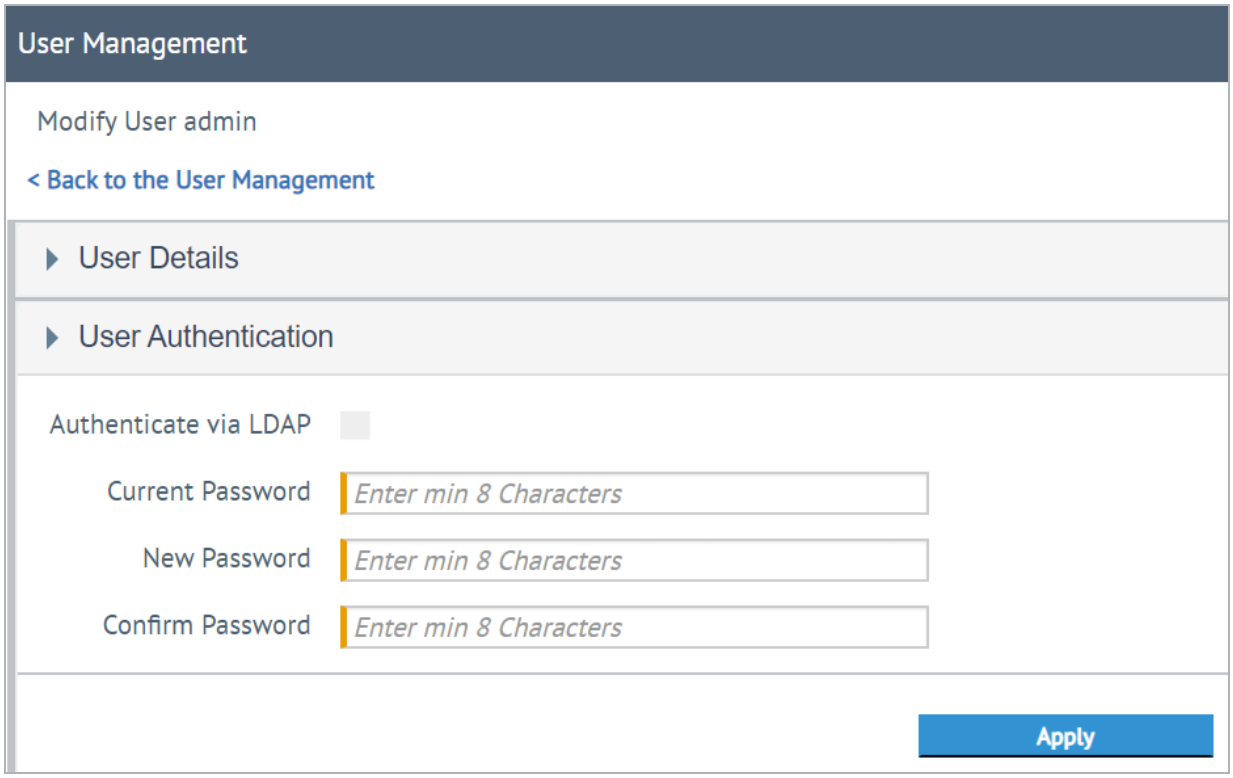
As an **admin** user, you can update your email address by typing your new email in the **Email** field and clicking **Apply**. You can update the usernames and email addresses of other users here also. You

do not need to know their current password. You can quickly activate/deactivate an account by selecting or clearing the **Active** button.

User Authentication

Users can use their Active Directory credentials to authenticate and log in to Kemp 360 Central. Tick the **Authenticate via LDAP** check box if you want the user to authenticate using their Active Directory credentials. For details on how to configure LDAP authentication in Kemp 360 Central, refer to the **Setting up LDAP Authentication** section.

> By updating your password, you also update the password for the console.

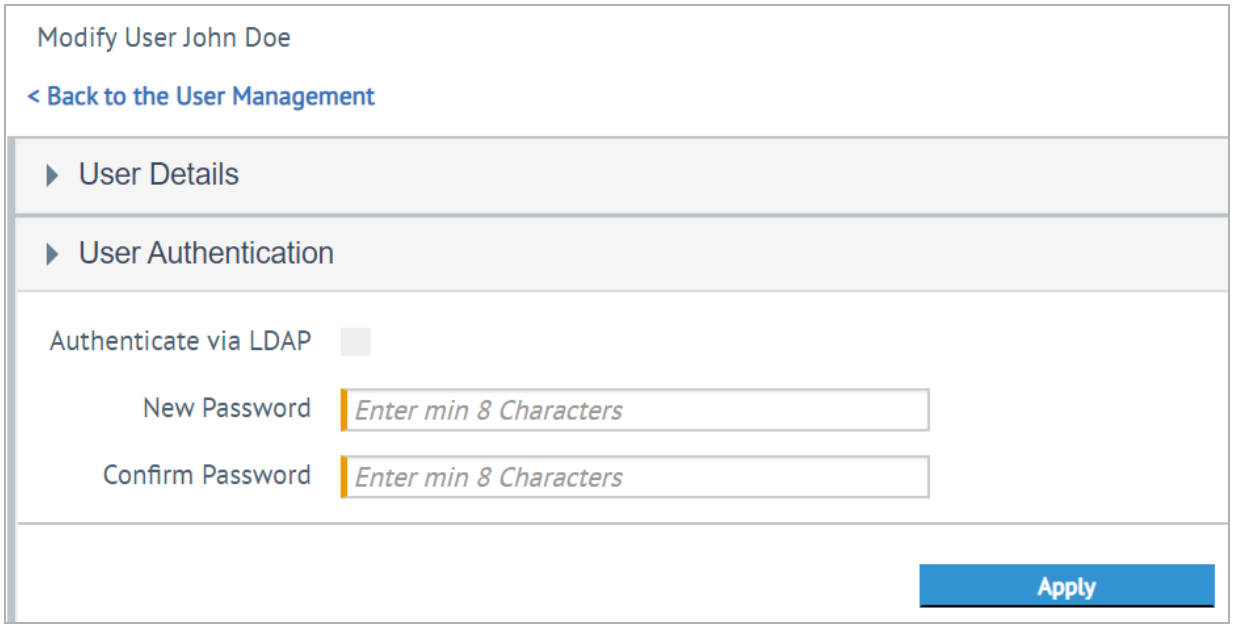


To update your password as an **admin** or non-admin user, perform the following steps:

1. Click the **User Authentication** section.
2. Type your current password in the **Current Password** field.
3. Type your new password in the **New Password** and **Confirm Password** fields.
4. Click **Apply**.

If the password is incorrect, a warning appears on screen.

If you update your password, your current login session is invalidated and you must log in again using your new password.

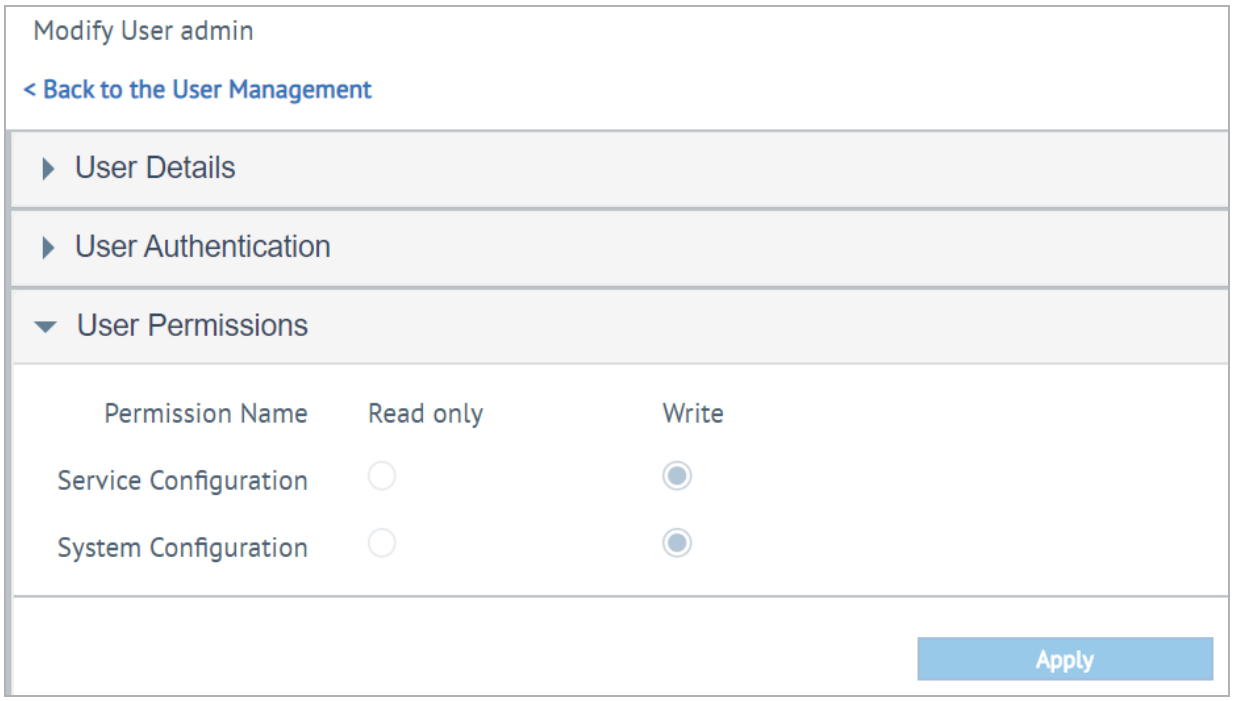


As an **admin** user, you can also reset the password of any user as follows:

1. Click the **Edit** icon of the user.
2. Click the **User Authentication** section.
3. Type the new password in the **New Password** and **Confirm Password** fields.
4. Click **Apply**.

As an **admin** user, you do not need to know the user's current password.

User Permissions

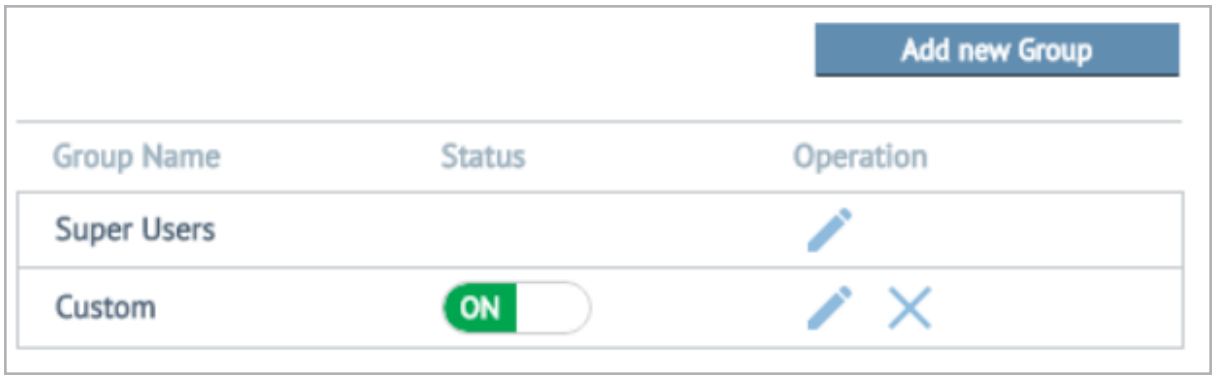


As an **admin** user, you can modify the user permissions of a user. The **User Permissions** are broken down by the main sections in Kemp 360 Central:

- **Service Configuration:** In the **Service Configuration** section, users perform various management tasks, such as adding, modifying, and removing Virtual Services, SubVSs, and Real Servers. Configure the user in a group to grant this level of access to individual devices and Virtual Services.
- **System Configuration:** The **System Configuration** section of Kemp 360 Central enables users to centrally manage LoadMasters. Other items that can be managed include: templates, firmware updates, reboots, backups, restorations, and syslog settings for any LoadMaster on a network.

12.2 Group Management

To access the **Group Management** screen, click the **Access Control** icon in the bottom-left of the screen and click **Group Management**.



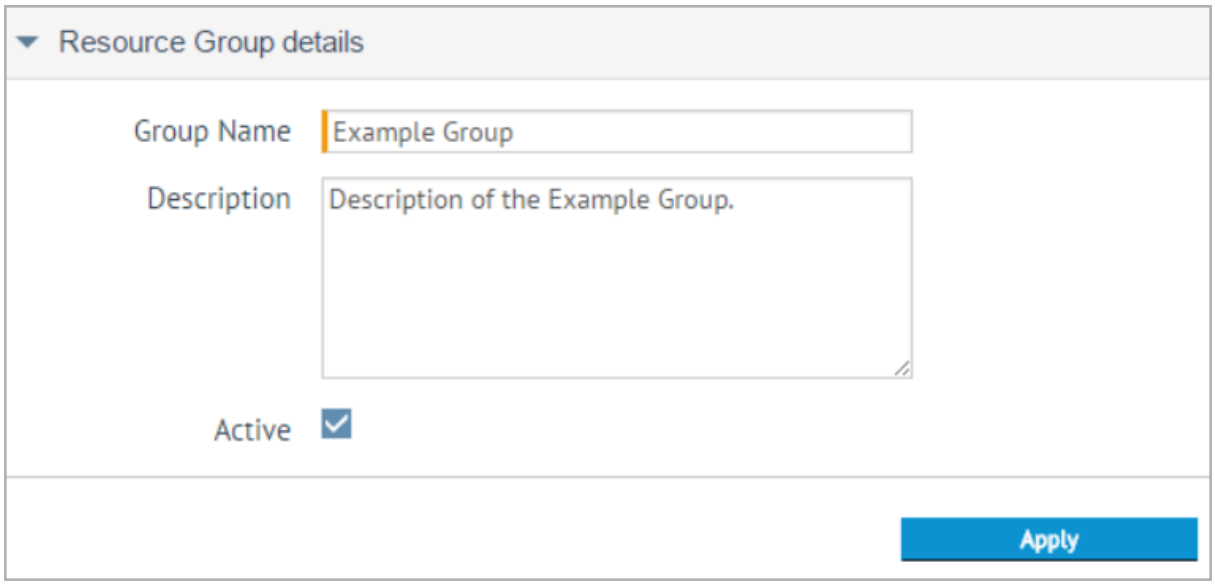
The **Group Management** screen lists any existing user groups. The **Super Users** group cannot be disabled or deleted because this is a default system group.

You can create a new group by clicking **Add new Group**.

The **Status** column shows whether the group is enabled or disabled. You can enable/disable a group by clicking the toggle button.

You can click the **Edit** (pencil) icon to edit a group or the **Delete** (X) icon to remove a group.

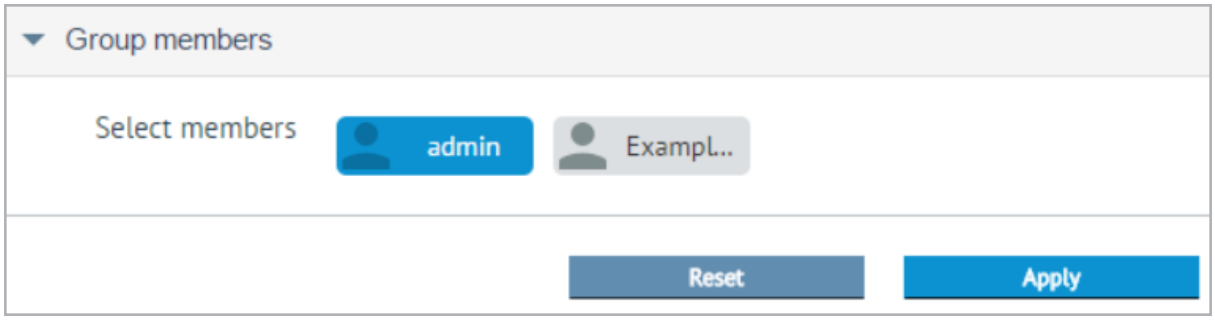
12.2.1 Group Details



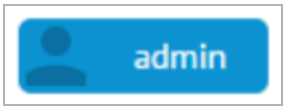
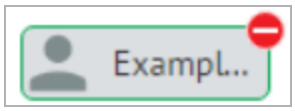
When adding a new group, you can specify the **Group Name**, a **Description** for the group and select whether or not to enable the group.

You can also change these settings for an existing group by modifying it.

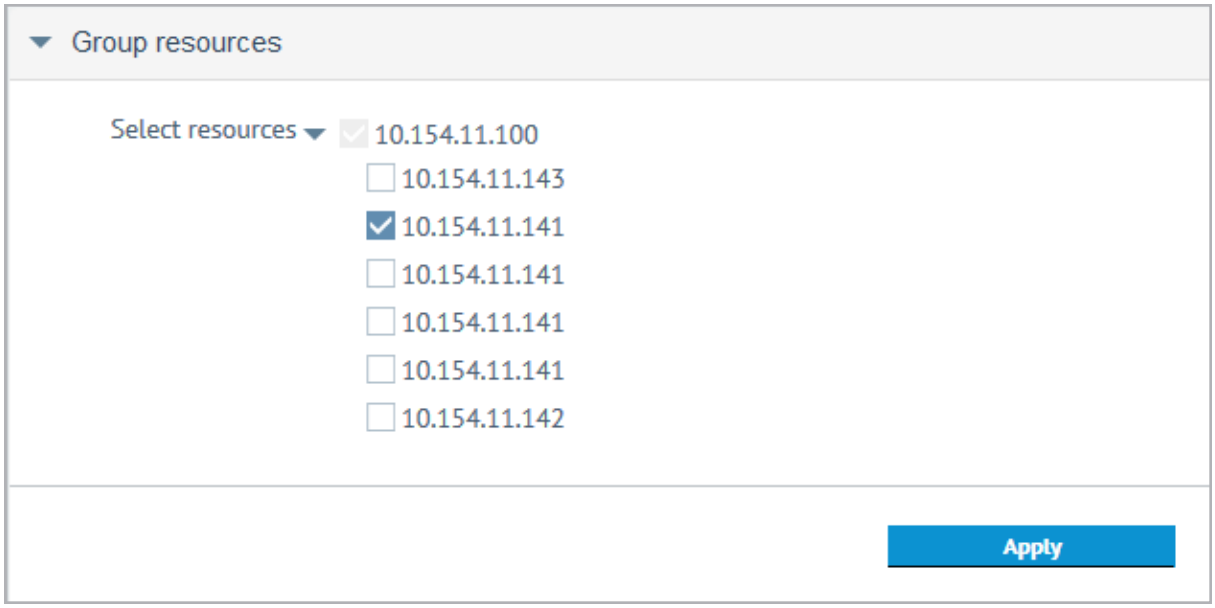
12.2.2 Group Members



When modifying a group, you can add and remove users to/from the group. To add or remove a user from the group, click the user listed to select them for addition/removal from the group. Different colors illustrate the status/operation. To remove any selection, click **Reset**. The table below provides a description of each color.

Color	Description
	The **admin** user is marked as blue because it is a member of all groups and cannot be removed.
	Grey users do not belong to the group.
	A green plus icon is displayed for users who have been selected to be added to the group.
	A dark green color indicates that the user is already a member of the group.
	The minus icon indicates a user who is a member of the group but has been selected to be removed from the group.

12.2.3 Group Resources



The **Group resources** section enables you to select what resources to give the group access to. The resources are listed by IP address. If a LoadMaster has Virtual Services, you can click the arrow to expand the list to see them. Select the relevant resources that you want to grant access to and click **Apply**. If a LoadMaster is not selected, but a Virtual Service underneath it is selected, the LoadMaster appears greyed out but selected in the display to indicate that something under it is selected.

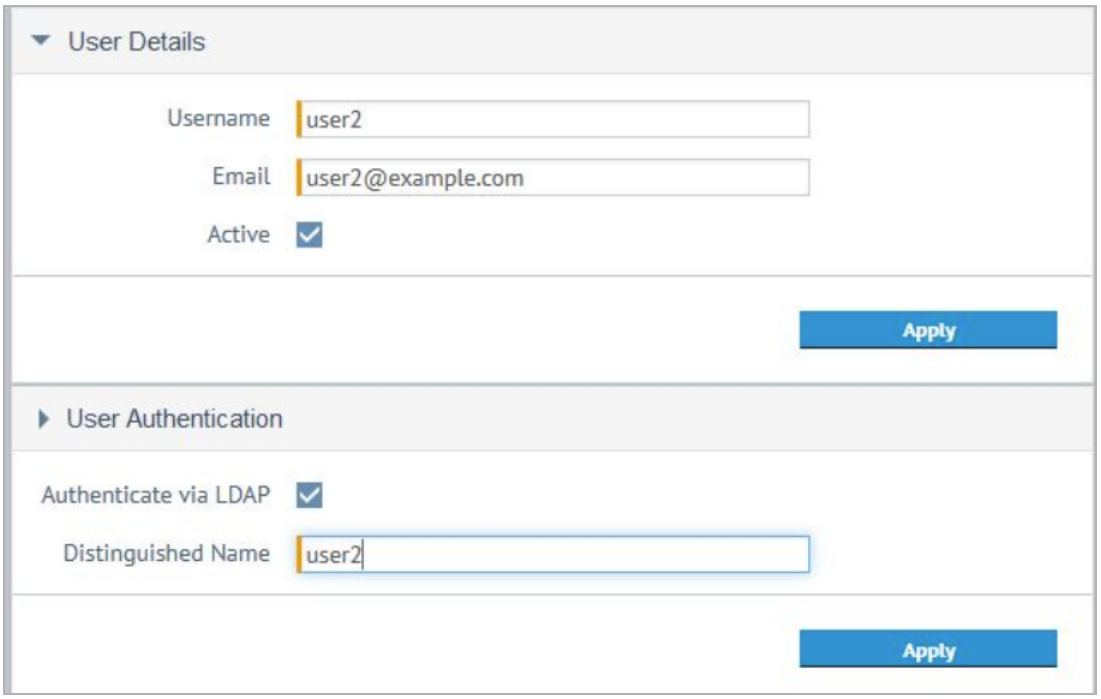
> It is recommended that you configure your shared IP, HA1, and HA2 into the same group.

12.3 Setting up LDAP Authentication

Users can use their Active Directory credentials to authenticate and log in to Kemp 360 Central.

To configure LDAP authentication, go to **Access Control > LDAP Authentication**. Here you must provide the required LDAP parameters.

You must add each user as a local user to establish their permissions.



When adding the local user you must enter the following information:

Username: Kemp recommends that you set this value the same as the LDAP login. If desired, this can be changed to other values.

Distinguished Name: This must be set to the LDAP username.

Authenticate via LDAP: This check box allows you to change between local authentication and LDAP. The username remains the same.

13 Network Settings

To access **Network Settings**, click the **Settings and Configuration** icon, then click **Network Settings**.

If DHCP settings are disabled on the console, as an **admin** user, you can set the default system DNS server using the UI. You can set a maximum of three DNS servers, which are queried in the order first, second, and third. You can remove a DNS server by clicking the minus icon then click **Apply**. You can reset all DNS settings by clicking **Unset**.

> If DHCP is enabled in the console, you are not able to manually change the DNS settings on the UI.

To configure the DNS settings, perform the following steps:

1. Type the IP address in the **DNS Server** field.
2. Click **Apply**.
3. Click the plus icon to add another DNS server.

14 Kemp 360 Central System Administration

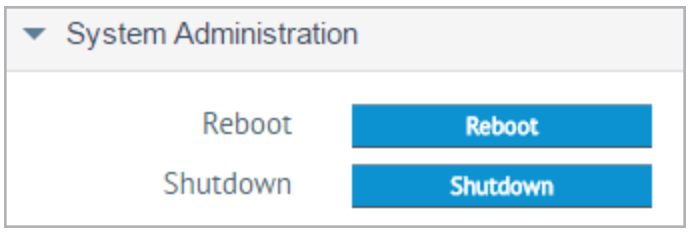
This section deals with the administration of the Kemp 360 Central instance, rather than with the administration of individual networks and LoadMasters.

A number of administration tasks can be performed in Kemp 360 Central.

To access the **Kemp 360 Central administration** section, click the cog icon in the bottom-left of the screen.

The settings in the figure above are explained in the following sections.

14.1 Reboot/Shutdown Kemp 360 Central



This section of the **System Administration** screen enables users to reboot or shut down the Kemp 360 Central instance.

When Kemp 360 Central is rebooted, it automatically attempts to re-connect to all previously configured LoadMasters. When rebooting, all settings are saved and take effect once the reboot is complete.

Clicking **Shutdown** powers down the Kemp 360 Central instance. After shutting down, the instance must be powered back on to turn the Kemp 360 Central instance back on. To power the instance back on, you must access the hypervisor or cloud platform where Kemp 360 Central is deployed. A shutdown of Kemp 360 Central does not affect the availability of the previously configured settings.

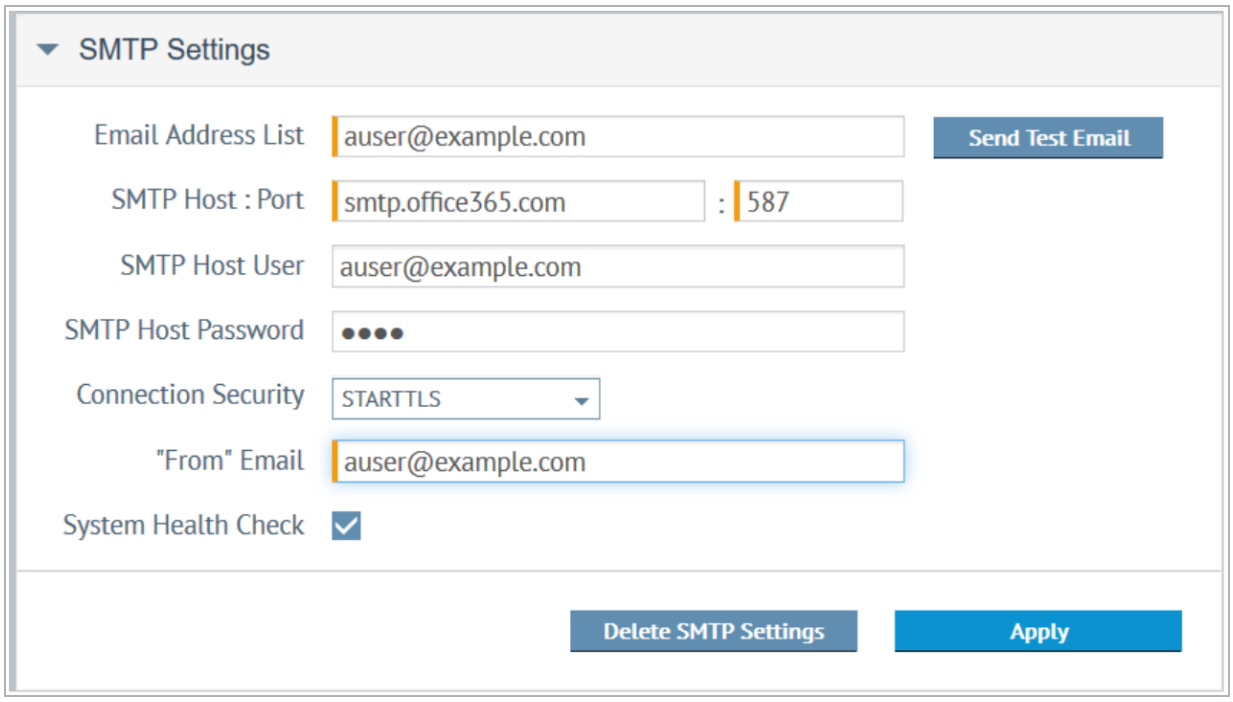
14.2 SMTP Settings

Configure SMTP to allow Kemp 360 Central to deliver email notifications to a user-defined email address list. There are a couple of prerequisites that must be in place for this to work:

- Kemp 360 Central must be able to reach the SMTP Host and SMTP Port specified.
- The SMTP Host User must be configured on the SMTP server.

Emails are sent when important events occur such as a device going down or becoming available again.

To configure the SMTP settings for Kemp 360 Central, follow the steps below:



1. Enter one or more email addresses in the **Email Address List** text box.

   Up to eight email addresses can be entered - separate multiple email addresses with semi-colons.

2. Enter the IP address of the SMTP Host to be used for sending email.
3. Enter the **port** used by the SMTP host.
4. Enter the **SMTP Host User** name used to log into the SMTP host.
5. Enter the **SMTP Host Password** for the user name specified above.

   At present, the **SMTP Host User** and **SMTP Host Password** fields are mandatory. If you do not want to specify a username or password - enter dummy details, save the settings, then clear those fields and save the settings again.

   Kemp recommends that a service account is used in the SMTP settings. Creating a specific service account for Kemp 360 Central avoids problems with passwords being changed on personal accounts and allows the capabilities for the service

account to be limited by the email system. Note that the SMTP password provided is not encrypted.

6. Select the **Connection Security** type. The choices are:

- **None** – email is sent using an unencrypted link
- **TLS/SSL** – email is sent using an encrypted link

7. Enter the email account from which Kemp 360 Central will send emails.

8. Clear the **System Health Check** check box if you do not want to receive notifications on system events and status.

With System Health Check enabled, the system sends email notifications on system events and status in the following scenarios.
If a LoadMaster availability changes form available to down or down to available, an email is sent to indicate the state change.
To prevent overloading of mailboxes with notifications, only a single notification is sent in any day (00:00 to 23:59).
The system does a self check at approximately 06:00 every day and an email notification is sent only if issues are detected.

9. Click the **Apply** button.

10. A test email can be sent by clicking the **Send Test Email** button. The Send Test Email button only appears after settings have been entered and the **Apply** button clicked.

14.3 Enable Temporary SSH Access for Diagnostic Purposes

In this section of the Kemp 360 Central UI, users can grant Kemp Support access to the Kemp 360 Central instance. SSH access to the Kemp 360 Central host can be enabled by the **admin** user with a once-off activation code provided by Kemp Support. **Remote SSH Access** is enabled by default, however, an admin can enable or disable **Remote SSH Access** by clicking the button to turn it on or off.

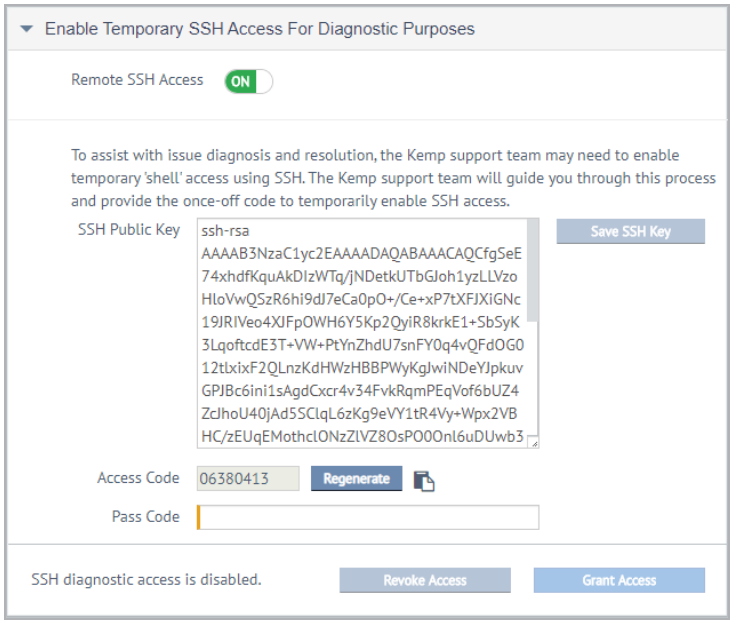
Users need both an SSH Public Key and an SSH access passcode as an SSH key pair is required to enable access.

Windows users should use PuTTY to generate a Public Key, while Unix users should use ssh-keygen.

1. Use PuTTY or ssh-keygen to generate an SSH Key.

2. Click the cog icon from the Kemp 360 Central menu.

3. Expand the **Enable temporary SSH access for diagnostic purposes** section. Initially, all the buttons are disabled.



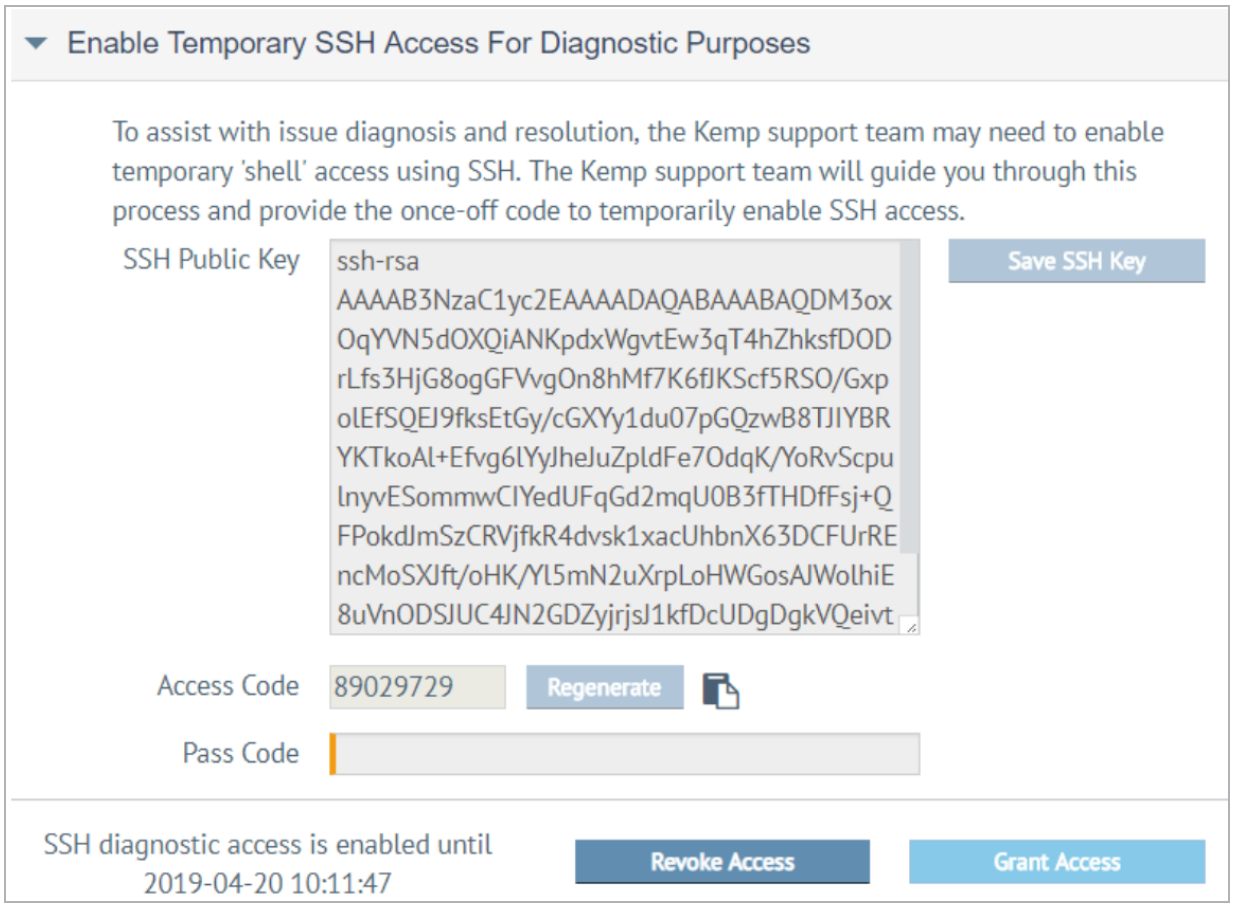
4. Enter an **SSH Public Key** code in the **SSH Public Key** text box. The **Save SSH Key** button is enabled.

5. Click **Save SSH Key**. The **Regenerate** button is now enabled.

6. To generate the access passcode, click **Regenerate**.

7. Contact Kemp Support and provide them with the generated passcode.

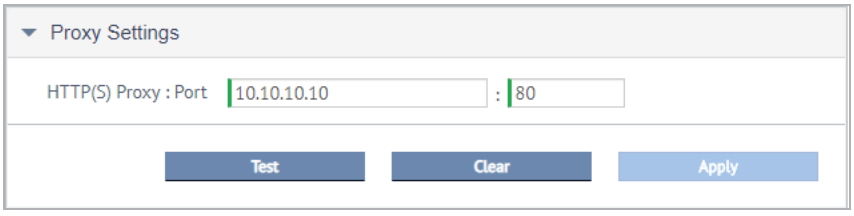
8. Kemp Support will provide you with a code that grants diagnostic SSH access.



9. Enter the code received from Kemp Support into the **Pass Code** text box and then click **Grant Access**. The text relating to the SSH diagnostic access updates to reflect the changes.

10. If you want to revoke access to the Kemp 360 Central instance, click **Revoke Access**.

14.4 Proxy Settings



Configuring the settings in this section enables Kemp 360 Central to access other networks using a HTTP(S) Proxy. When you specify either an IP address or a fully qualified domain name (FQDN) and a port into the text boxes shown above, the **Apply** button becomes active. Click **Apply** to apply the

changes. The **Test** button now becomes active. After the parameters are set, click the **Test** button to check if the proxy server is reachable. To clear any data, click **Clear**.

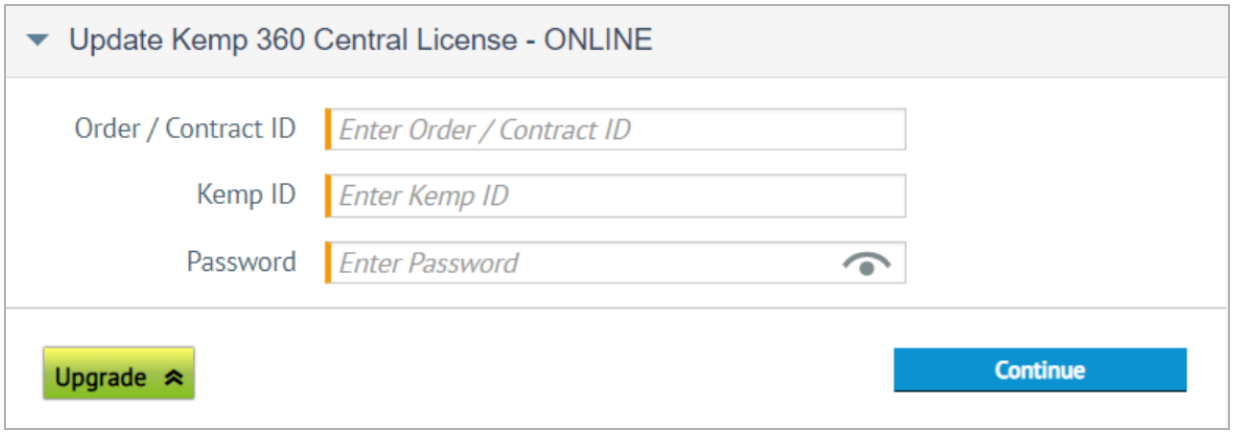
The IP address or FQDN and port you enter must point at a working HTTPS proxy that relays packets to another network with internet access, so that Kemp 360 Central can use the proxy to communicate with Kemp.

15 License Management

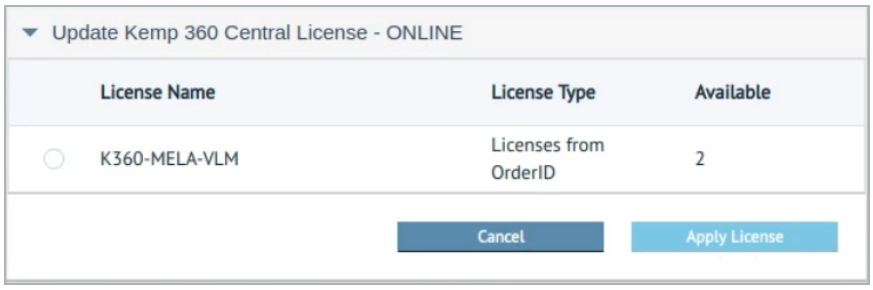
The Kemp 360 Central license can be updated, if required. This would be required if, for example, you upgrade to premium support or you want to move from a trial license to a permanent license.

To update your Kemp 360 Central license, complete the following steps:

1. In the bottom-left corner, click the cog icon.
2. Click **License Management**.
3. You can use online or offline licensing to update the Kemp 360 Central license.



If you are upgrading during a trial, type your **Order** or **Contract ID** in the field provided, along with your **Kemp ID** and **Password**, and click **Continue**.



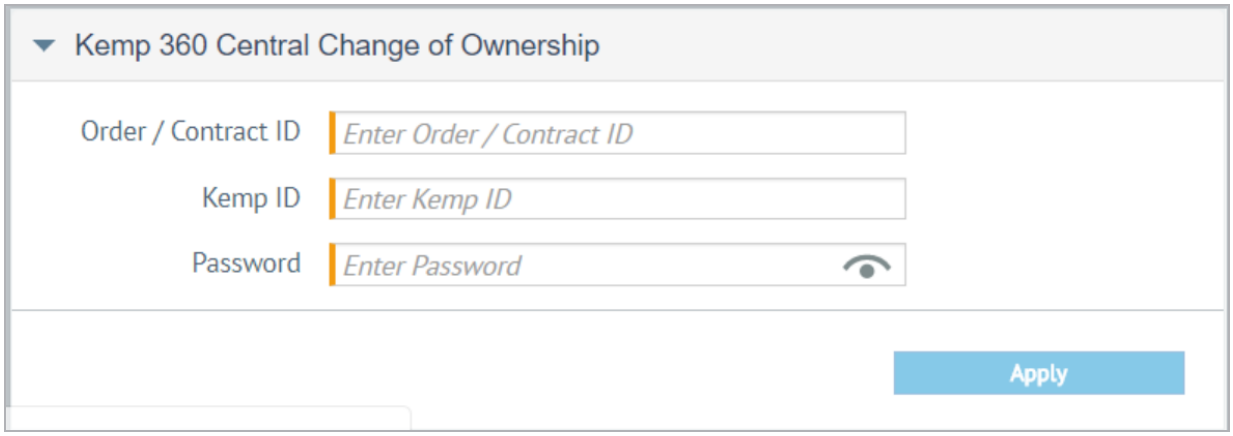
Click **Apply License** to apply the license.

> If you do not want to apply the license, click **Cancel** to return to the previous screen.

After successfully licensing, a message displays saying the license has been updated. The license information can be viewed by clicking the help icon in the bottom-left of the screen and going to the **About** page.

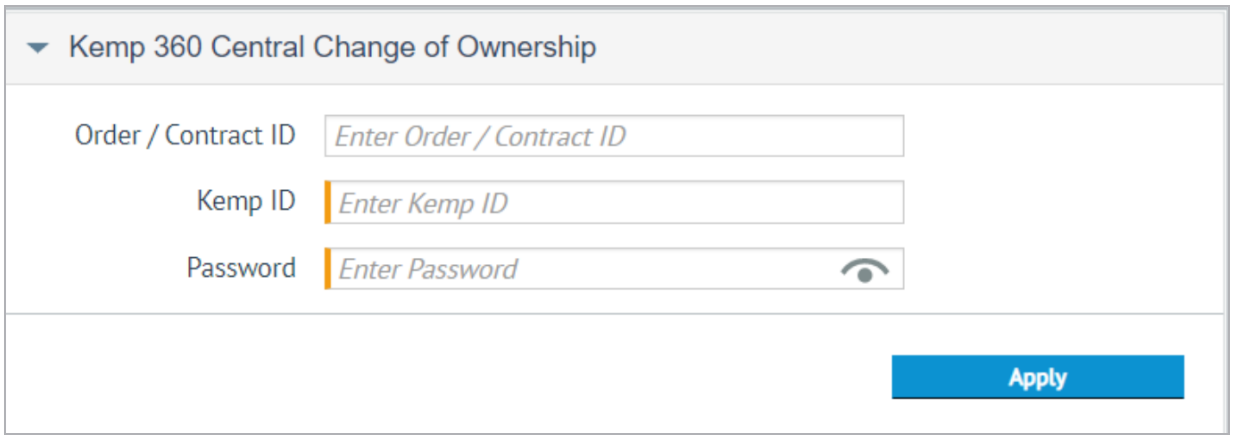
Change of Ownership

If the **admin** user has to be changed to another user, you can transfer ownership of the license using the **Change of Ownership** functionality.



If you want to transfer ownership of your Kemp 360 Central instance to another user, type your **Order** or **Contract ID** used to license the machine initially along with the **Kemp ID** and **Password** of the user you want to assign the license to and click **Apply**.

> If you do not enter an Order or Contract ID on a machine that was licensed with an Order or Contract ID, you receive a warning.



If your version of Kemp 360 Central was licensed without an Order or Contract ID, you do not need to complete the **Order / Contract ID** field. Type your Kemp ID and password in the fields provided and click **Apply.**

You cannot change ownership with a trial license.

16 Update System Software

You can update the Kemp 360 Central firmware using the **Update System Software** screen. You can check the current firmware version by clicking the question mark icon in the bottom-left of the Kemp 360 Central UI.

> After updating the firmware – Kemp 360 Central must be rebooted.

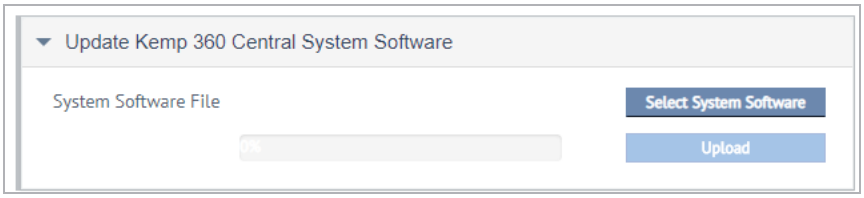
A firmware update patch file is required to update the firmware offline. Contact Kemp Support to get the patch file.

> Online updates are not supported. You must download the patch file from Kemp to the system you use to access the Kemp 360 Central UI and then upload the patch through the UI.

To update the Kemp 360 Central firmware, follow the steps below:

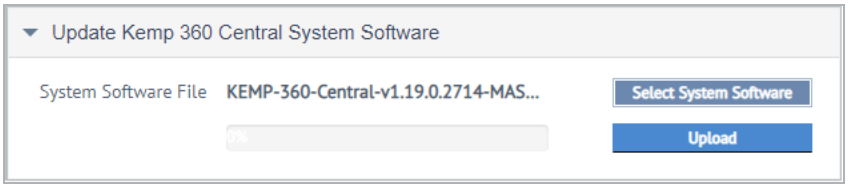
1. In the Kemp 360 Central UI, click the cog icon in the bottom-left corner.

2. Click **Update System Software**.

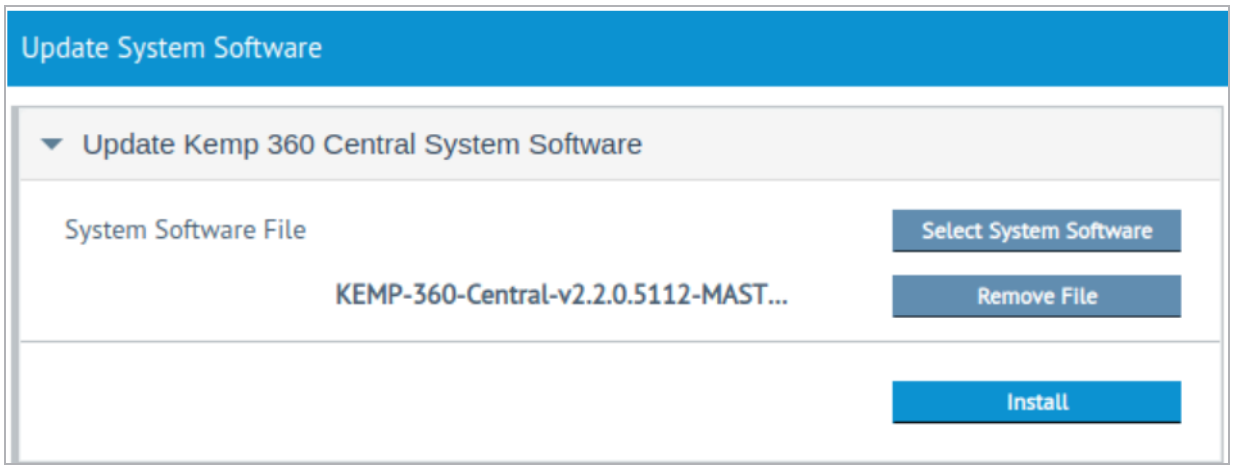


3. Click **Select System Software**.

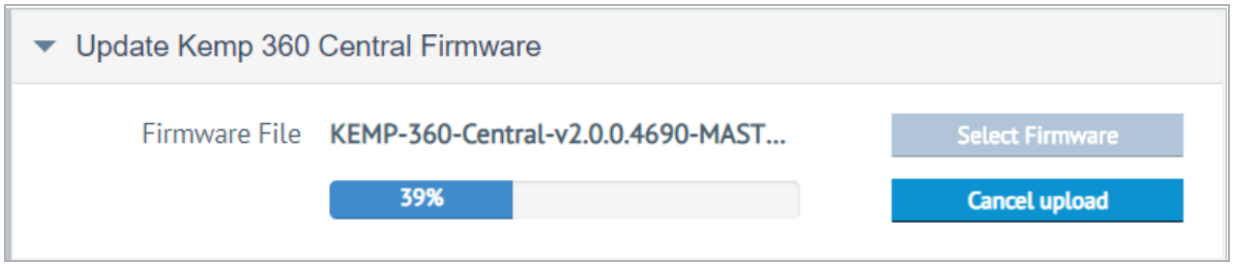
4. Browse to and select the firmware update file.

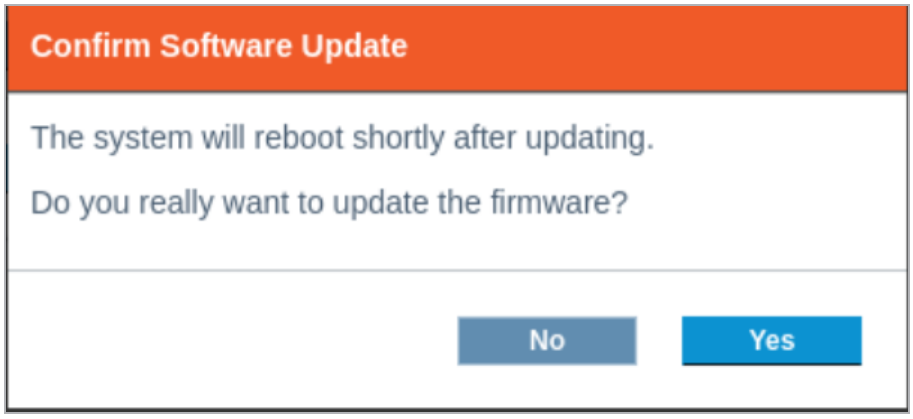


5. Click **Upload**. Once the image is uploaded to Kemp 360 Central, the **Install** button appears.



6. Click **Install** to continue.

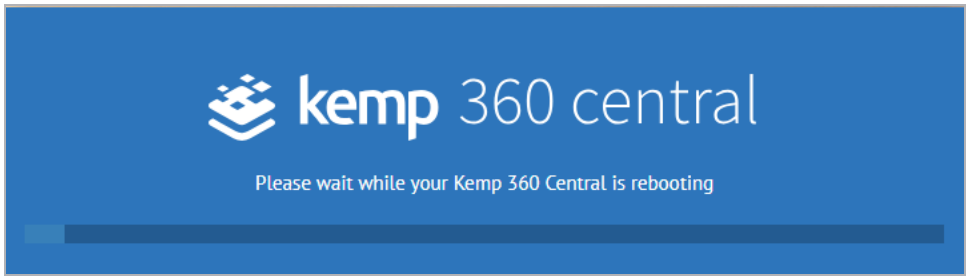




7. Upgrading the system firmware requires a system reboot after the update is applied. Click **Yes** to continue the upgrade or click **No** to cancel.

Kemp 360 Central now runs a self-test as part of the firmware upgrade. If the self-test fails, an email is sent (based on SMTP configuration) and cancels the upgrade process. If no SMTP is

configured, you can view the process details in the System log file. Since Version 1.23, we have improved the logging of the firmware upgrade process.



You can view the progress of the upload in the progress bar.

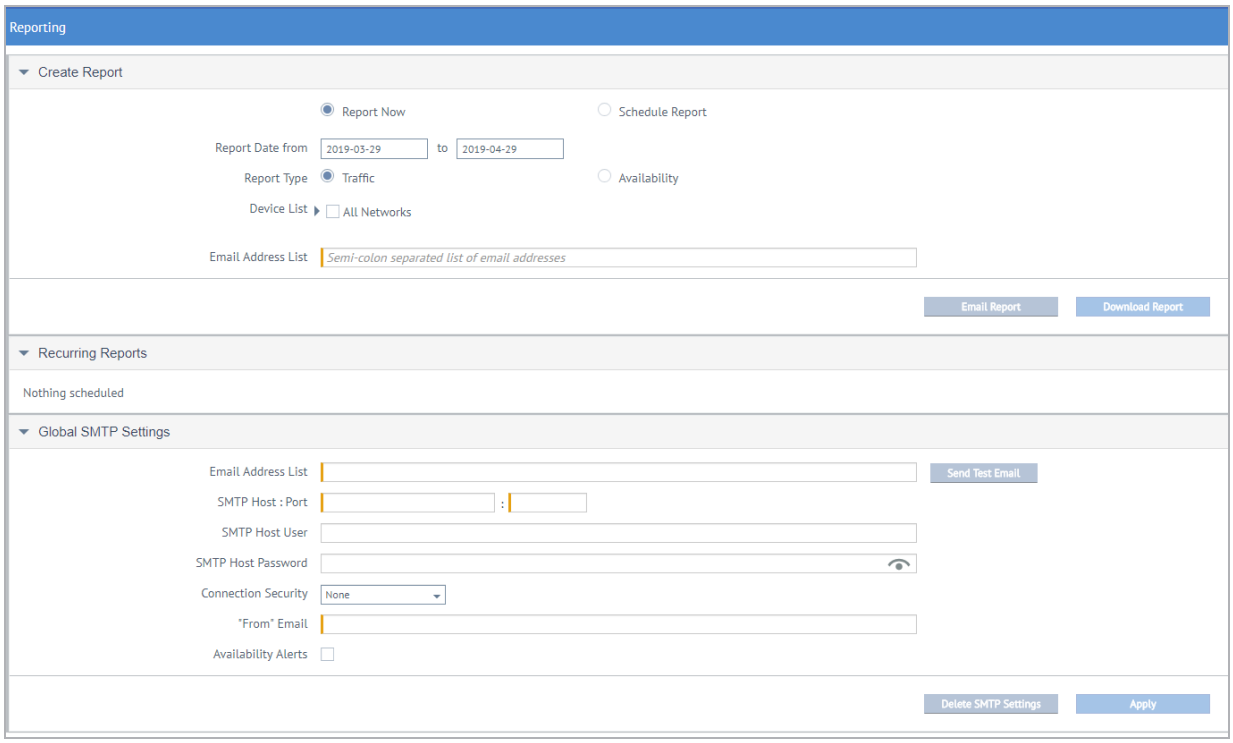
8. After the update, Kemp 360 Central reboots. If you either get an error message during the upgrade process or the system is still running the same release after upgrade, check the system log (click **Settings and Configuration > Log Files**) for any related messages during the time period that you attempted the upgrade.

Do not make any further attempt to use the UI until the system has automatically rebooted, which takes a few minutes. After completing the update, the login screen is displayed.

Since version 1.19, if you try to navigate away from this screen while the system is updating, the **Under Maintenance** page appears until the upgrade is complete.

17 Reporting

To open the **Reporting** section, click the **Settings and Configuration** icon then click **Reporting**. There are three sections within Reporting: **Create Report**, **Recurring Reports** and **Global SMTP Settings**.



17.1 Create Report

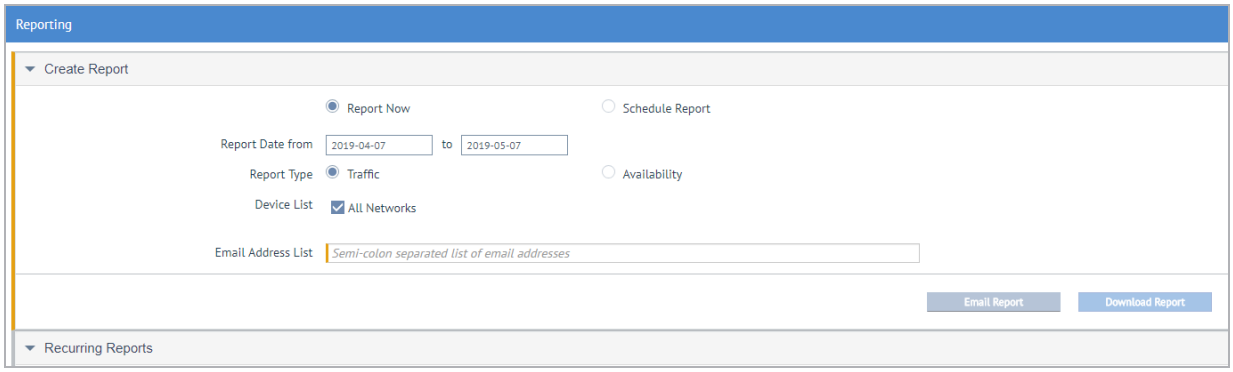
The controls in this feature enable you to specify either:

- An on-demand report that is prepared immediately and that you can then either download locally or email to specific recipients
- A scheduled report that is run periodically at a specified interval and then emailed to specific recipients
- An Availability PDF report for selected devices

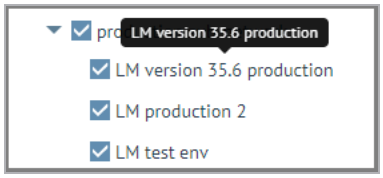
> Note that if you want to email a report, the SMTP Settings (see the section below) must be provided beforehand.

To create an on-demand report, perform the following steps:

1. Select the **Report Now** radio button (selected by default).
2. Use the **Report Date** controls to specify the time period for the report.



3. Use the check boxes in the **Devices** list to select the devices that will appear in the report. You can select **All Networks** if you want to include all networks. If you select a network node, all the devices in that network are included.



> Hovering over a device name in the **Create Report** section displays the full nickname for the device.

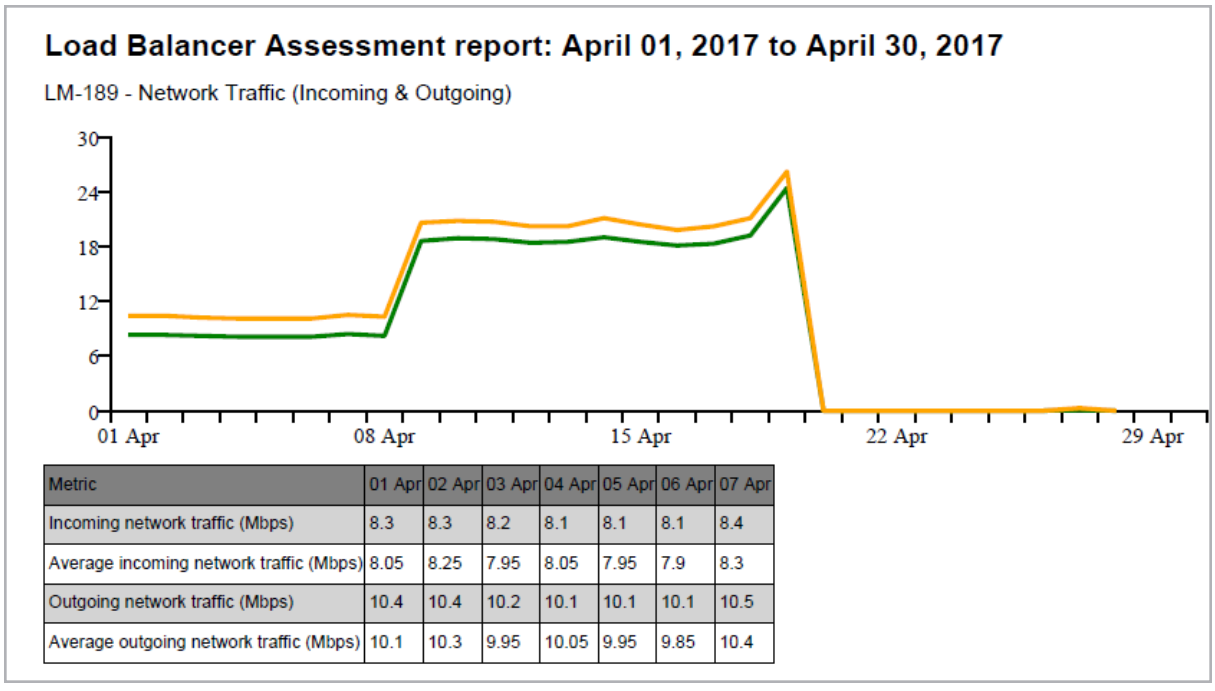
4. Do one of the following:
   - To download the report as a PDF file, click **Download Report**.
   - To email the report, check that the **SMTP Settings** are set, type a list of email addresses separated by semicolons (;) into the **Email Address List**, and click **Email Report**. A popup is displayed and a system message is logged indicating whether or not the email was sent successfully.

To schedule a report for some time in the future, perform the following steps:

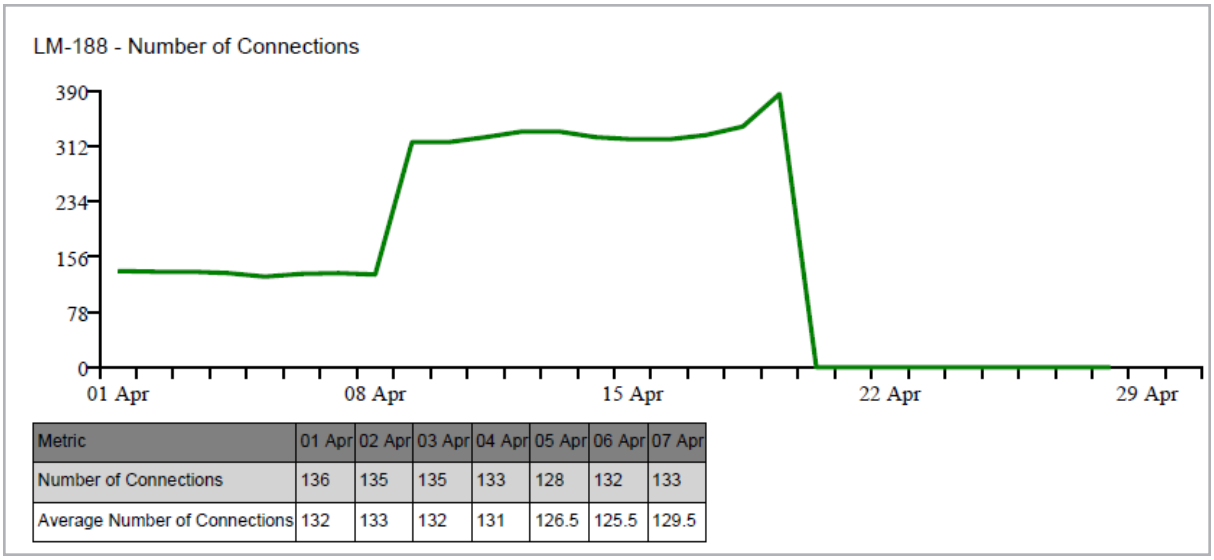
1. Select the **Schedule Report** radio button.
2. Select the **Report Type** from the drop-down list. This can be daily, weekly or monthly. The start time and date of the report is set to 00:00:00 on the next full day, week, or month. For example, if today is Wednesday and you select **Weekly**, the report's first run will be on the following Monday at 00:00:00.
3. Use the check boxes in the **Device** list to select the devices that appear in the report. To select all networks, select the **All Networks** check box. If you select a network node, all the devices in that network are included.
4. Type a list of email addresses separated by semicolons (;) into the **Email Address List**.
5. Click **Create Schedule**. A notification appears informing you that you successfully created the scheduled report.

The name of the report is a Load Balancer Assessment report and it contains the following graphs:

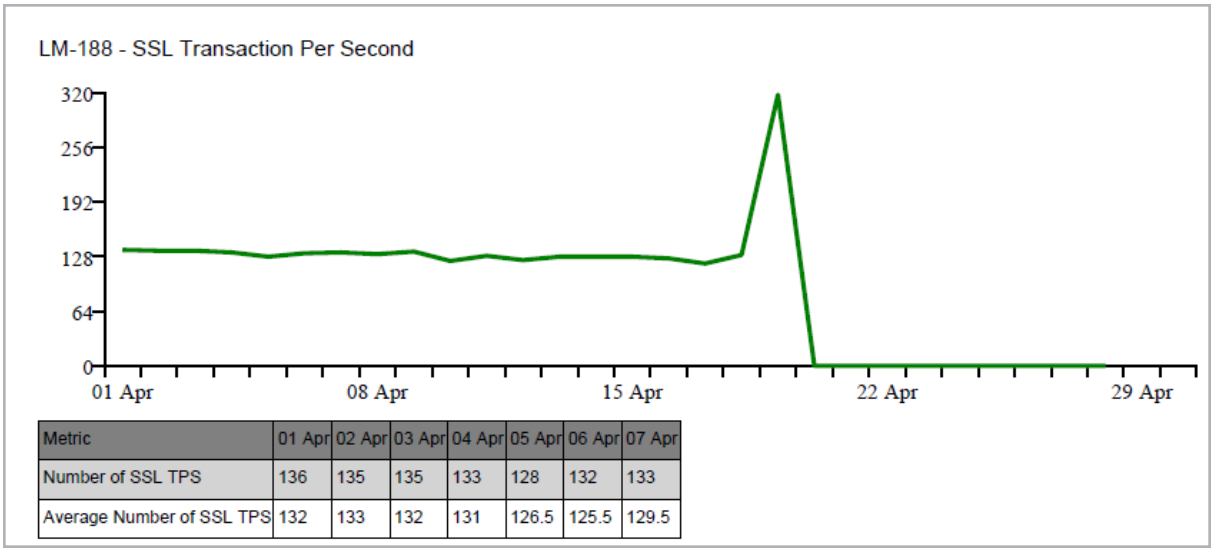
- Network Traffic (Incoming & Outgoing)
- Number of Connections
- SSL Transaction Per Second



Metric	01 Apr	02 Apr	03 Apr	04 Apr	05 Apr	06 Apr	07 Apr
Incoming network traffic (Mbps)	8.3	8.3	8.2	8.1	8.1	8.1	8.4
Average incoming network traffic (Mbps)	8.05	8.25	7.95	8.05	7.95	7.9	8.3
Outgoing network traffic (Mbps)	10.4	10.4	10.2	10.1	10.1	10.1	10.5
Average outgoing network traffic (Mbps)	10.1	10.3	9.95	10.05	9.95	9.85	10.4



Metric	01 Apr	02 Apr	03 Apr	04 Apr	05 Apr	06 Apr	07 Apr
Number of Connections	136	135	135	133	128	132	133
Average Number of Connections	132	133	132	131	126.5	125.5	129.5



Metric	01 Apr	02 Apr	03 Apr	04 Apr	05 Apr	06 Apr	07 Apr
Number of SSL TPS	136	135	135	133	128	132	133
Average Number of SSL TPS	132	133	132	131	126.5	125.5	129.5

The diagrams above show examples of the different reports. The table under the graph provides more details depending on the report.

To create an Availability report, perform the following steps:

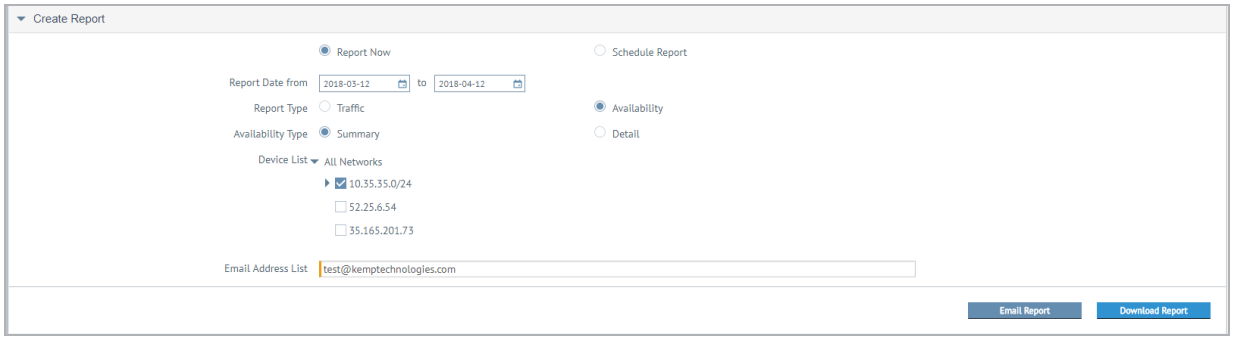
5. Select **Availability** as the Report type then select either **Summary** or **Detail**.

- Summary is the default report type
- Detail provides more information

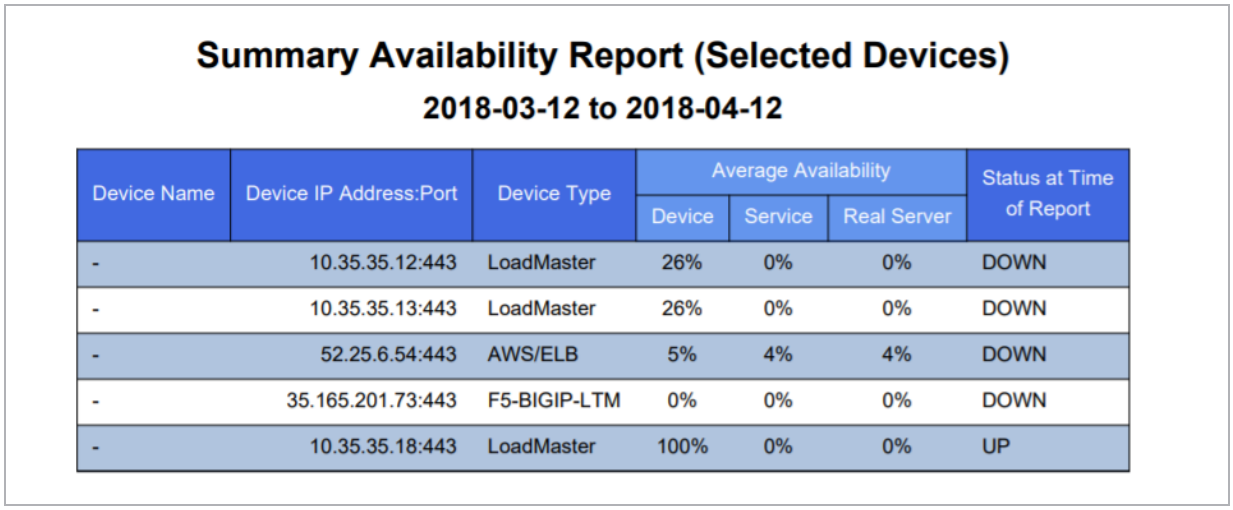
6. Select the devices you want to run the report for.

7. To send the report by email, type an email address in the **Email Address List** field and click **Email Report**.

8. To download the report, click **Download Report**.



Summary Report



Summary Availability Report (Selected Devices)

2018-03-12 to 2018-04-12

Device Name	Device IP Address:Port	Device Type	Average Availability			Status at Time of Report
			Device	Service	Real Server	
-	10.35.35.12:443	LoadMaster	26%	0%	0%	DOWN
-	10.35.35.13:443	LoadMaster	26%	0%	0%	DOWN
-	52.25.6.54:443	AWS/ELB	5%	4%	4%	DOWN
-	35.165.201.73:443	F5-BIGIP-LTM	0%	0%	0%	DOWN
-	10.35.35.18:443	LoadMaster	100%	0%	0%	UP

The Summary report displays a tabulated picture of each device's availability. It contains the following columns:

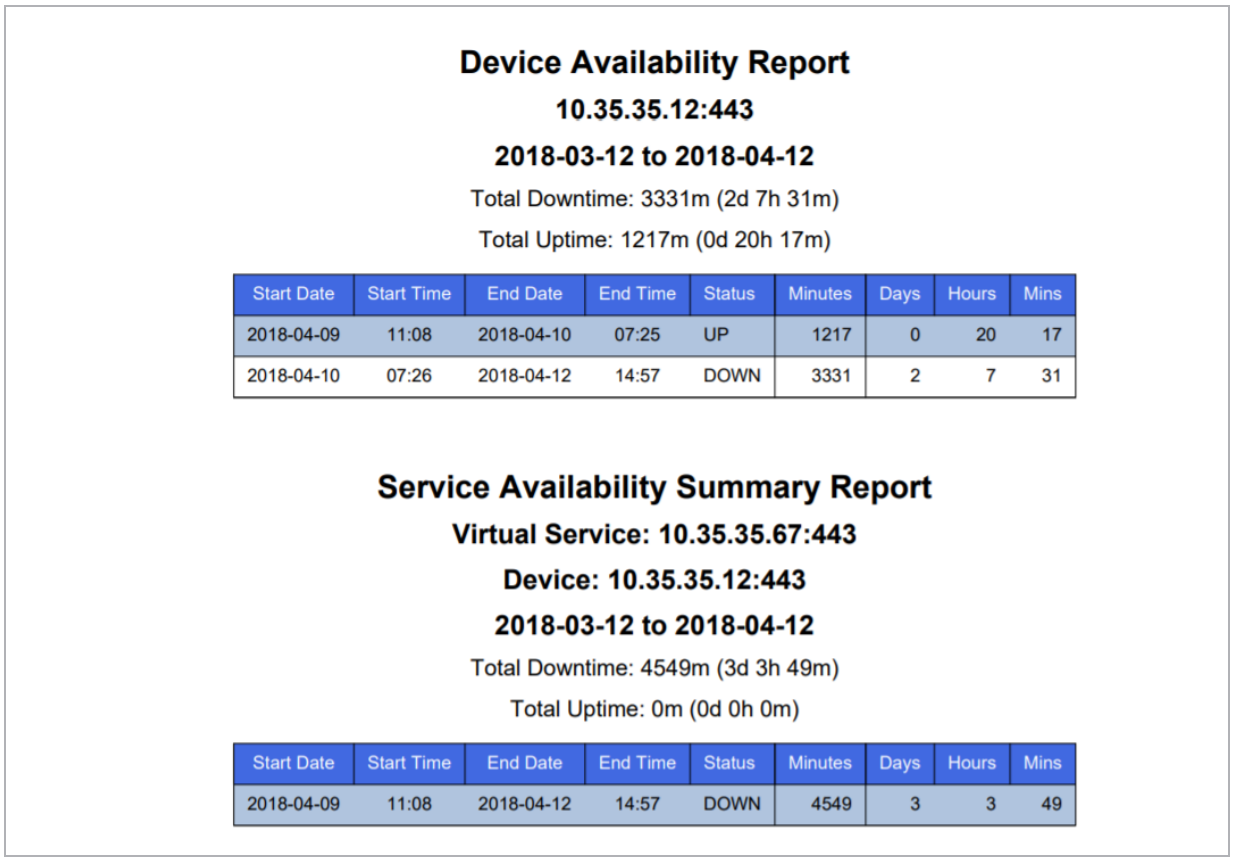
- **Device Name**: Displays the device nickname. If there is no nickname, a dash is displayed instead.
- **Device IP Address:Port**: Displays the IP address and the port number of each device.
- **Device Type**: Lists the types of devices.

- **Average Availability**:
  - **Device**: Displays the average percent of time that the device was working.
  - **Service**: Displays the average percent of time that the Service was working. This value cannot be greater than the device value because it is possible that some of the services were down.
  - **Real Server**: Displays the average percent of time that the Real Server was working.
- **Status at Time of Report**: Indicates if the device was up or down at the time the report was run.

> If a device is not supported, it appears as 0% in the table.

Detail Report

The Detail report is broken down into two sections; the **Device Availability Report** and the **Service Availability Summary Report**.



Device Availability Report

10.35.35.12:443

2018-03-12 to 2018-04-12

Total Downtime: 3331m (2d 7h 31m)

Total Uptime: 1217m (0d 20h 17m)

Start Date	Start Time	End Date	End Time	Status	Minutes	Days	Hours	Mins
2018-04-09	11:08	2018-04-10	07:25	UP	1217	0	20	17
2018-04-10	07:26	2018-04-12	14:57	DOWN	3331	2	7	31

Service Availability Summary Report

Virtual Service: 10.35.35.67:443

Device: 10.35.35.12:443

2018-03-12 to 2018-04-12

Total Downtime: 4549m (3d 3h 49m)

Total Uptime: 0m (0d 0h 0m)

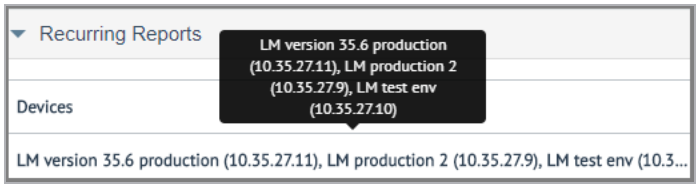
Start Date	Start Time	End Date	End Time	Status	Minutes	Days	Hours	Mins
2018-04-09	11:08	2018-04-12	14:57	DOWN	4549	3	3	49

The **Device Availability Report** displays the total downtime and total uptime of each device you run the report for. It also contains a table that displays the uptime and downtime in alternate rows including the specific date and time from when the device was working until the date and time the device went down. The next row then displays the same information for when the device was down and so on. It also displays this time period in total minutes and then breaks it down into days, hours, and minutes.

> You can also display the same data for sub-Virtual Services and third-party devices.

17.2 Recurring Reports

All previously created reports are listed in the order they were created. The table lists the first 128 characters of the device list, followed by the next run date, the frequency of the report, and the last run status (if applicable). Use the control at the right side of the table to delete a report.



Hovering over a device name in the **Recurring Reports** section displays the full nickname for the device.

17.3 Global SMTP Settings

This section shows the **Global SMTP Settings**, which are required to be set if you are emailing a report or sending the report will fail. Note that these are the same settings as shown under **Settings and Configuration > SMTP Settings** and **About and Help > Welcome On Board > SMTP Settings**.

Note that the email address list specified in the **Global SMTP Settings** does not apply to emailed reports. Reports are emailed only to the recipient list specified when creating the report.

This feature is an important component for emailing reports and is covered in more detail in the **SMTP Settings** section.

18 LoadMaster Licensing from Kemp 360 Central

This section displays local licensing information and metrics data on LoadMasters under the control of Kemp 360 Central. The license you have determines what you can see and what reports you can generate. For example, if you have a Metered license, the UI displays the sum of the peak usage of all active devices licensed for metered usage. This is calculated as the sum of the peak usage of all active devices licensed for metered usage.

However, if you have a Pooled license, you are allocated a specific amount of storage space and you can add or delete LoadMasters while staying within this limit. The UI displays how much of your license pool you are using out of your limit.

> If you have SMTP configured, you are notified by email if you exceed the allowed limit. This email is generated at midnight every day until the issue is fixed.

You can return a license to the license pool by going to the **Actions** column and clicking **Recover License**. This kills the device and returns the capacity to the license pool.

> You must also delete this LoadMaster from your hypervisor or cloud environment.

To access the **LoadMaster Licensing** section, click the **Settings and Configuration** icon then click **LoadMaster Licensing**.

> You can have a Pooled license or a Metered license but not both.

The information you obtain from running a report depends on whether you have a Metered or Pooled license. This is explained in the sections below.

18.1 Metered Usage Report

The **Metered Usage Report** zip file is downloaded by selecting the appropriate month and clicking **Export**. You can use the filter provided on the UI to filter results by device name or IP address to

make the report more specific. This CSV file contains day-by-day data of peak usage for that calendar month (measured in Gb).

> For the current month, the data is accurate up until the time the report is exported.

18.2 Pool Usage Report

The **Pool Usage** report displays the details that are displayed in the table in report format. However, you can filter on IP address or device name to make the report more specific. The report is downloaded as a .CSV file. The CSV file contains a history of all pooled device license actions for all devices.

18.3 Network Requirements for Local Licensing

LoadMaster devices that are issued a license from Kemp 360 Central must be able to communicate with the Kemp 360 Central server through port 443 to maintain the license validity. Each LoadMaster licensed by Kemp 360 Central validates their license daily. If validation fails, the LoadMaster enters a 30-day grace period after which the license expires. A successful validation resets the license to normal.

If SMTP services are configured and the LoadMaster is unable to contact Kemp 360 Central for 20 days, the system sends an email notification daily corresponding to the devices that have failed to validate their license.

> It is recommended that you configure SMTP to enable delivery of notifications of systems that are failing.

19 License a LoadMaster with a Local License

Kemp 360 Central can locally license LoadMaster instances when a Metered or Pooled license is applied.

19.1 Licensing Devices

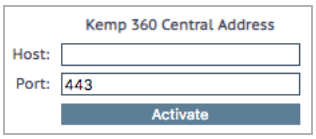
With Kemp 360 Central local licensing functionality, it is possible to license a number of LoadMasters locally using Kemp 360 Central - without the need to contact the Kemp licensing server.

When you initially deploy a locally licensed-enabled LoadMaster, a **Kemp 360 Central Activation Settings** screen appears. Enter the details for Kemp 360 Central. The LoadMaster then contacts Kemp 360 Central to license the LoadMaster. Following licensing, the LoadMaster must be activated in Kemp 360 Central. Detailed, step-by-step instructions are provided in the following sections.

> Local activation only works with specific VLM builds known as SPLA builds. Contact Kemp Support to access the VLM build for your local license instance.

19.1.1 License a LoadMaster using Kemp 360 Central

When an SPLA LoadMaster is initially deployed, you must select **Kemp 360 Central Licensing** (formerly Local Activation on pre-7.2.43 LoadMasters) or **Online Licensing**.



When a locally licensed LoadMaster is initially deployed, a screen (similar to the one above) appears. If this screen does not appear, you are not using the correct version of the LoadMaster. Contact a Kemp representative if this is the case.

The Kemp 360 Central (with local licensing enabled) details must be configured in the LoadMaster web User Interface (UI) so the LoadMaster can contact Kemp 360 Central. Follow the steps below to activate the LoadMaster:

1. Type the **Host** details of Kemp 360 Central in the **Host** text box.
2. Type the **Port** to access Kemp 360 Central on in the **Port** text box.

   > The internal IP address and host name can be found in the **Dashboard** screen of the Kemp 360 Central instance. The hostname is based on the instance name, which is specified when originally creating the instance. If you are not using Azure, the default hostname is **K360Central**.

3. Click **Activate**. The available license types are displayed.
4. Select the relevant license type and click **Continue**.

The LoadMaster is now licensed against Kemp 360 Central, thus using one of the available licenses.

19.1.2 Activate the LoadMaster in Kemp 360 Central

After completing the steps in the previous section, the LoadMaster is now licensed.

The LoadMaster periodically checks for the presence of the locally activated license (Kemp 360 Central). If the locally activated license cannot be found, or there are any errors, an error message is displayed and the VLM stops working after a predetermined length of time based on your agreement with Kemp. If an activation check fails, an error message appears on the LoadMaster home screen indicating that activation failed.

The association between a LoadMaster and a license in Kemp 360 Central depends on the LoadMaster's MAC address on the interface on which the administrative IP address of the LoadMaster resides. In most hypervisors, it is possible to modify the MAC address of a VM; this should be avoided by disabling MAC address changes in the hypervisor.

If the MAC address of a LoadMaster that obtained its license from Kemp 360 Central changes, the following occurs:

- The LoadMaster is no longer recognized by Kemp 360 Central as having a valid license; it enters its licensing renewal grace period after its next daily attempt to contact Kemp 360 Central.
- Attempts to license the LoadMaster again are refused by Kemp 360 Central because a managed device at the LoadMaster's IP and port already exists in the device tree.

The workaround is to:

1. Remove the existing LoadMaster device from Kemp 360 Central by selecting it in the device tree and clicking the delete (minus) icon at the lower left of the UI.
2. Opening the LoadMaster WUI and requesting a new license from Kemp 360 Central.

19.2 Deregistering a LoadMaster

LoadMaster licenses can be deregistered and removed permanently if needed.

> Kemp recommends taking a backup of the LoadMaster configuration before deregistering it. Manual backups can be taken by going to **System Configuration > System Administration > Backup/Restore** in the main menu of the LoadMaster web UI, or by going to cloud icon > **System Configuration > Backup/Restore** in the Kemp 360 Central interface.

When a LoadMaster is deregistered, it frees up another instance to be registered. For example, if you have reached the LoadMaster limit (local license limit) and you deregister one LoadMaster, you can now activate another LoadMaster.

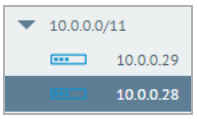
There are two ways to deregister the LoadMaster - using Kemp 360 Central or using the LoadMaster. Refer to the relevant section below for step-by-step instructions.

> Kemp strongly recommends deregistering a LoadMaster using the Kemp 360 Central UI, rather than the LoadMaster UI. Deregistering a LoadMaster from the LoadMaster UI can lead to the LoadMaster having an unknown state in Kemp 360 Central. In these cases, it is not easy to remove the LoadMaster from Kemp 360 Central and the unknown LoadMaster is still taking up an available license.

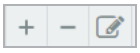
19.2.1 Deregister using Kemp 360 Central

To deregister a LoadMaster using Kemp 360 Central, complete the following steps:

1. Click the cloud icon on the left.



2. Select the LoadMaster to be removed.



3. Click the remove button (minus icon) in the bottom-left.

4. Click **Yes** to the warning message that appears.

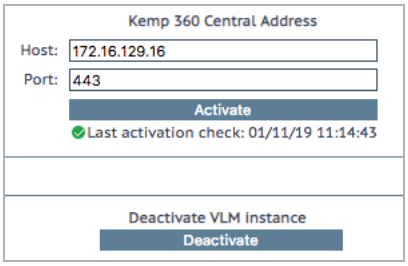
5. The LoadMaster instance is rebooted and returns to the **Kemp 360 Central Activation Settings** screen when it comes back up.

6. There is now an available, free license instance, which can be viewed on the **System Administration** page. This is because an active license has been removed.

19.2.2 Deactivate using the LoadMaster UI

Follow the steps below in the relevant VLM web UI to deregister it:

1. In the main menu, go to **System Configuration > Miscellaneous Options > Kemp 360 Central Activation Settings**.



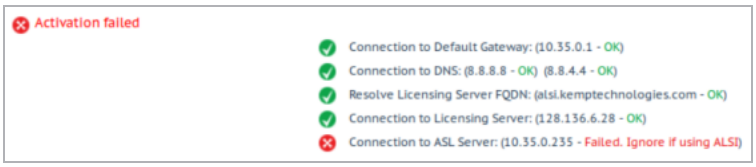
2. Click **Deactivate**.

3. When the license is killed, the VLM automatically reboots. After the reboot, the VLM is unlicensed and the **Licensing** screen appears. You can re-license the LoadMaster by selecting either **Online Licensing** or **Kemp 360 Central Licensing**.

The LoadMaster is also removed from any Kemp 360 Central monitored networks it is attached to. There is now an available, free license instance in the local license pool. This is because an active license has been removed.

19.3 Troubleshooting

If you try to license and there are any issues, a number of checks are performed automatically and the results and associated error message are displayed.



These checks perform the following tasks:

- Ping Default Gateway
- Ping DNS Servers
- Ping Licensing Server
- Ping Activation Server

You can also manually check the Kemp 360 Central debug log. If there are no entries relating to local licensing, it means the connection to Kemp 360 Central has failed.

> Kemp 360 Central notifies you if there are disk space issues that prevent normal operation, and you should contact Kemp support immediately to resolve those issues. Note that while deploying a new Kemp 360 Central instance and applying a previously created backup can also bring your configuration back online, you will lose all statistics and log data by re-deploying in this manner. The best practice is to contact Kemp Support even if you do re-deploy, so that support personnel can attempt to remedy your issues and recover historical data.

19.4 Troubleshooting Local Licensing

When a LoadMaster is successfully activated by Kemp 360 Central, a log message that looks like the following is added to the audit log:

```
Activating ASL instance 172.16.188.1 with ASL License VLM-MAX. Current
activations is 5
```


The current activation is per license type and not the total number of all active instances. When a LoadMaster is successfully re-licensed by Kemp 360 Central, two log messages that are similar to the ones below are added to the audit log:

```
ASL Instance 172.16.188.1 license change. Old license was VLM-MAX and current activations is 4
```

```
Activating ASL instance 172.16.188.1 with ASL License VLM-5000G. Current activations is 2
```

Similarly, the current activation is per license type. The first log message refers to old licenses and the next refers to the new license type. When an activation failure is observed on the LoadMaster ASL Activation page, the reason for the failure can be determined by looking at the debug log on Kemp 360 Central as shown below:

Debug Log Message	Description
ASL instance limit already reached. Cannot issue more licenses	Kemp 360 Central has already activated the maximum number of LoadMasters permitted. To activate another LoadMaster, you must de-activate a currently activated LoadMaster or contact Kemp to obtain a new license that increases the number of LoadMasters that Kemp 360 Central can activate.
ASL License given by lic_type_id <integrer> does not meet the requirements.	An internal error occurred; contact customer support.
No message in debug log and also no message of successful activation in audit log.	The activation request was refused because Kemp 360 Central is not configured to provide licenses that match the LoadMaster's platform type.
Cannot verify ASL instance check. Is the request really coming from a LoadMaster?	This occurs if Kemp 360 Central is unable to verify whether the request came from a LoadMaster or something else. The LoadMaster sends specific headers in its requests.

19.5 Comparing Metered Licensing Reports to Other Network Graphs and Reports

There is a data discrepancy between the **Network Metrics** graphs and the **Metered Licensing Report for Peak Throughput**. This is because:

- The network graphs on the Monitoring tab and in the reports available from **Settings and Configuration > Reporting** generate network metrics based on throughput recorded on all the network interfaces on the LoadMaster. This includes the entire packet size transfer in or out of the LoadMaster (IP header, TCP header, and TCP segment transferred in or out of the LoadMaster).
- The graphs and reports also includes TCP overhead such as plain ACK, connection establishment, termination, retransmission, and so on.
- For the Metered Licensing reports available under **Settings and Configuration > Metered Licensing Management**, only the maximum throughput of data transfer for Virtual Services is recorded. This only accounts for application data (HTTP request/response in case of HTTP transactions) transferred for all the Virtual Services. This does not include any TCP overhead to transmit the data.
- For a single transaction, there are approximately equal amounts of traffic between the client and Virtual Server and between the Virtual Server and the Real Server. The network interface accounts for both sides of traffic but for Virtual Service data transfer (billed in Metered Licensing), only application data transfer between the client and the Virtual Server is recorded.

> Because of this, the statistics reported in the graphs is much higher than statistics reported for Metered Licensing purposes. There is no direct relation between them because it depends on the traffic flow.

20 Scheduled Actions

In this section, users can view, edit, and delete all scheduled actions across all LoadMasters in the Kemp 360 Central inventory.

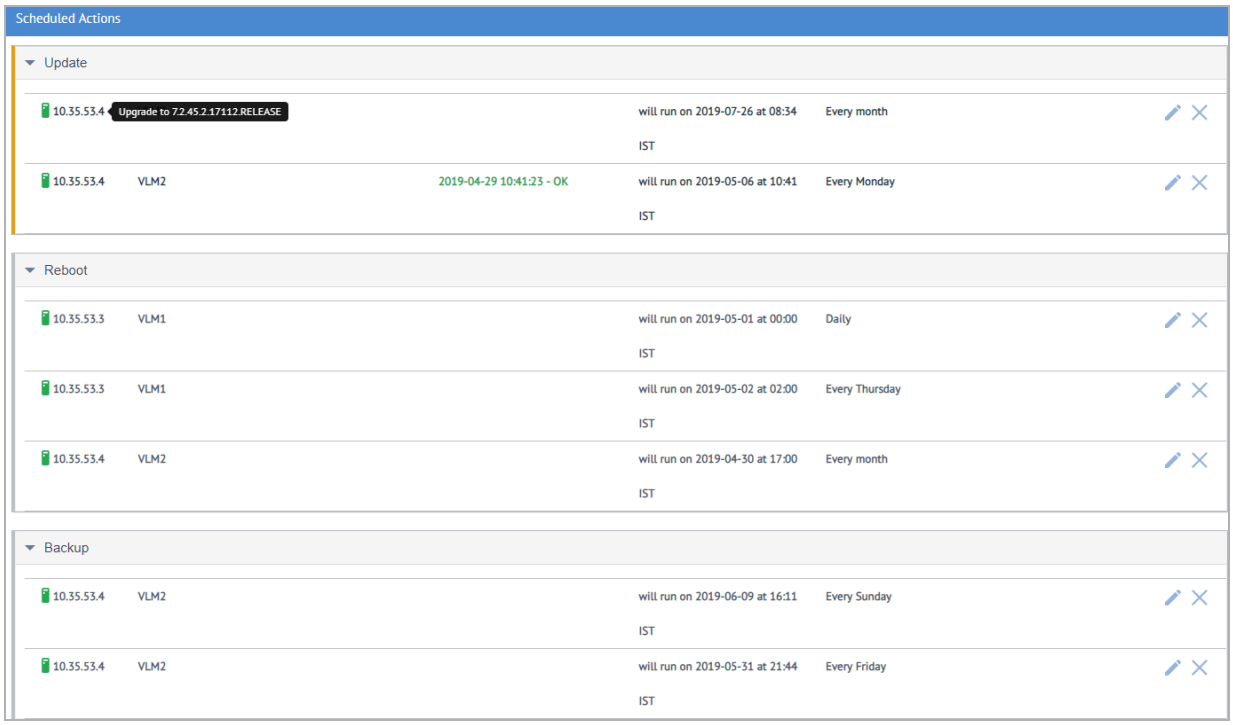
For LoadMasters configured into LoadMaster HA Pairs, you can only schedule an upgrade on the individual LoadMasters in the pair, and not on the HA Shared IP device.

> Any LoadMaster that is scheduled to be backed up will not work on a new machine when restored because the firmware of the LoadMaster is not backed up.

20.1 View Scheduled Actions

To view scheduled actions on a Kemp 360 Central instance, complete the following steps:

1. Click the cog icon on the left of the screen.
2. Click **Scheduled Actions**.

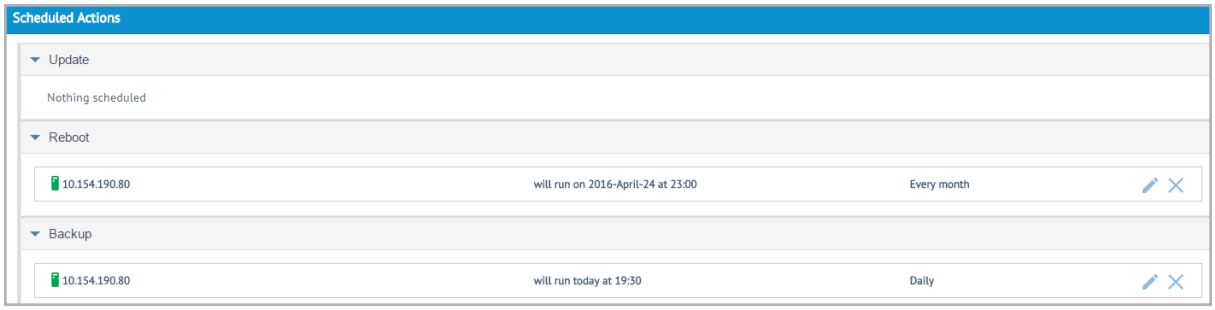


A full list of scheduled firmware updates, reboots, and backups displays. To display details of the firmware you are updating to, hover your mouse over the IP address.

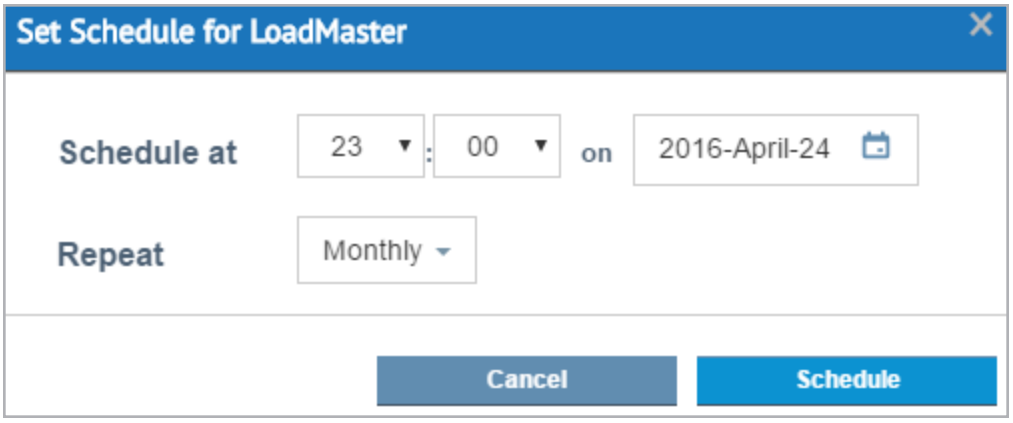
20.2 Modify Scheduled Actions

To make changes to scheduled actions, complete the following steps:

- 1. Click the cog icon on the left of the screen.
- 2. Click **Scheduled Actions**.



3. Click the edit icon of the scheduled action you wish to modify.



4. Make changes, as required, to the scheduled settings.

> Tasks cannot be scheduled within one hour of each other.

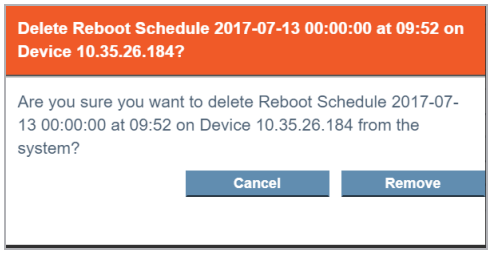
20.3 Delete a Scheduled Action

To delete a scheduled action, complete the following steps:

1. Click the cog icon on the left of the screen.

2. Click **Scheduled Actions**.

3. Click the delete icon of the scheduled action you wish to discontinue.



4. If you want to proceed, click **Remove** on the toaster message that appears.

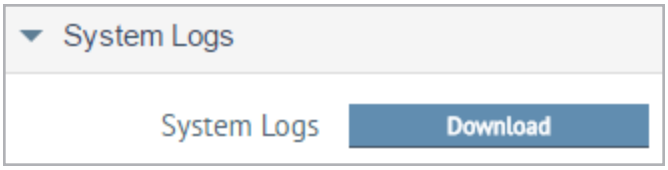
21 Log Files

To access the Kemp 360 Central log files, click the **Settings and configuration** icon in the bottom-left of the screen and click **Log Files**.

In this section of the Kemp 360 Central UI, users can download l Kemp 360 Central logs.

21.1 System Logs

The **System Logs** file includes Kemp 360 Central system logs.

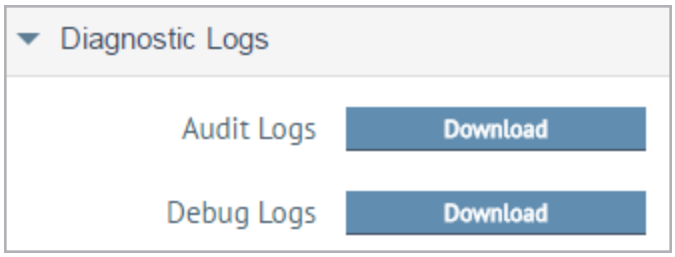


Perform the following steps to download the Kemp 360 Central system logs:

1. In the menu, click the **Settings and configuration** icon and then click **Log Files**.
2. Click the **Download** button next to System Logs. Your browser now displays a popup that enables you to view the downloaded logs using a local application of your choice or save the logs.

21.2 Diagnostic Logs

In this section, users can download both **Audit Logs** and **Debug Logs**.



Use these logs as diagnostic tools when a problem has occurred. When the **Download** button is clicked, the logs download as a text file.

The **Audit Logs** display application logs, that is logs of actions completed in Kemp 360 Central, for example, adding a LoadMaster.

The **Debug Logs** are lower-level than the **Audit Logs**. The **Debug Logs** show logs relating to the application.

21.3 Log Settings

LoadMasters generate various warning and error messages using the syslog protocol. These messages are normally stored locally in the LoadMaster. Kemp 360 Central automatically configures the system log options for the LoadMasters to store the LoadMaster system logs in Kemp 360 Central.

To view the LoadMaster logs, go to the **Global Repository** and click **Logging**. For further information, refer to the **Logging** section.

For instructions on how to configure the syslog options, refer to the following section.

22 Date and Time

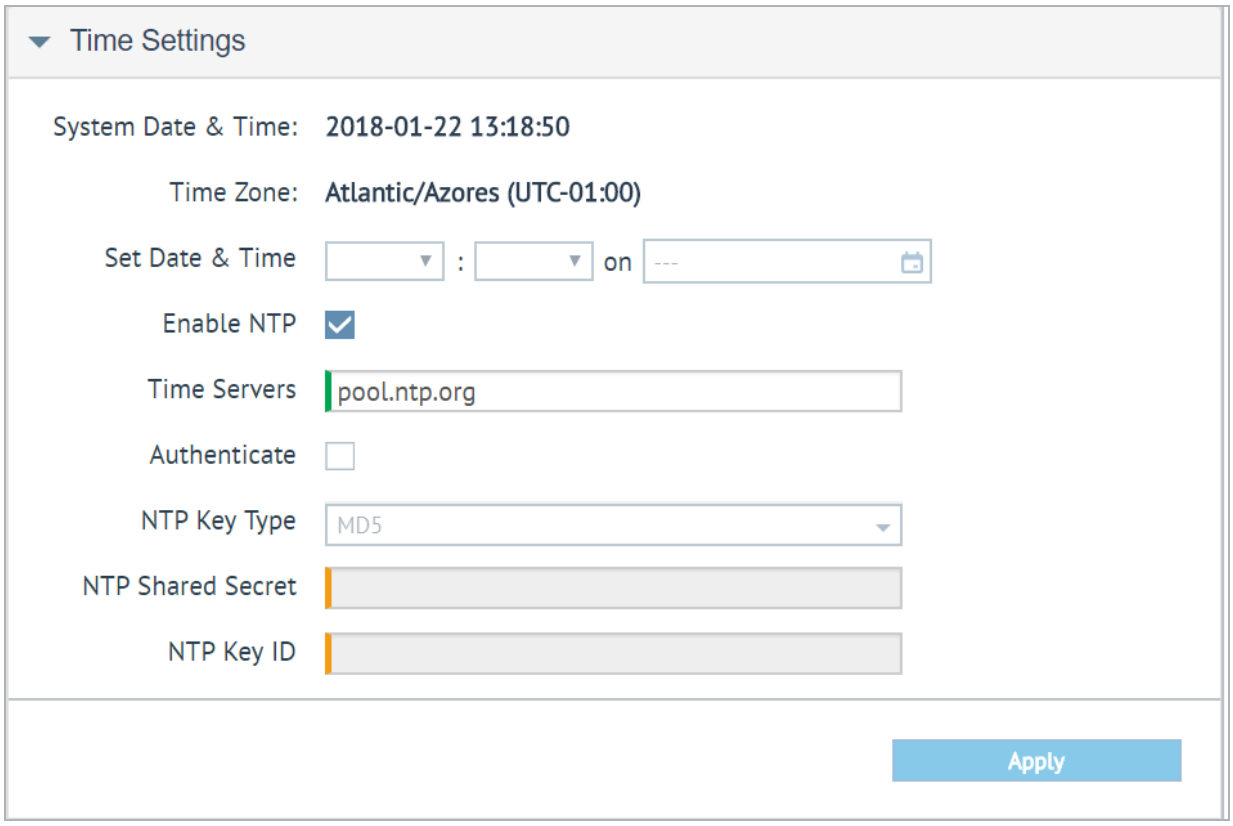
If there is a discrepancy in the time on your version of Kemp 360 Central, this can cause issues such as Metered Licensing reports not being sent on time and other scheduled tasks being executed at unexpected times. To mitigate against this, when you upgrade your version of Kemp 360 Central to Version 1.21 or deploy a new version, Network Time Protocol (NTP) synchronization is enabled by default.

The date and time appears on the top right of the User Interface (UI). To view the current time settings, click the **Settings and Configuration** icon then click **Date & Time**.

To automatically set the time using an NTP server (enabled by default), select the **Enable NTP** check box and click **Apply**. The machine automatically synchronizes its time with an NTP server (pool.ntp.org is used by default). Kemp 360 Central checks every hour (35 minutes past the hour) and after reboots, to check if there is any discrepancy between the local time and the NTP server. If there is a discrepancy, Kemp 360 Central updates according to the time of the NTP server being used. If the NTP server fails or goes down at any time, a warning notification appears on the UI to the left of the time when the scheduled contact is not made.

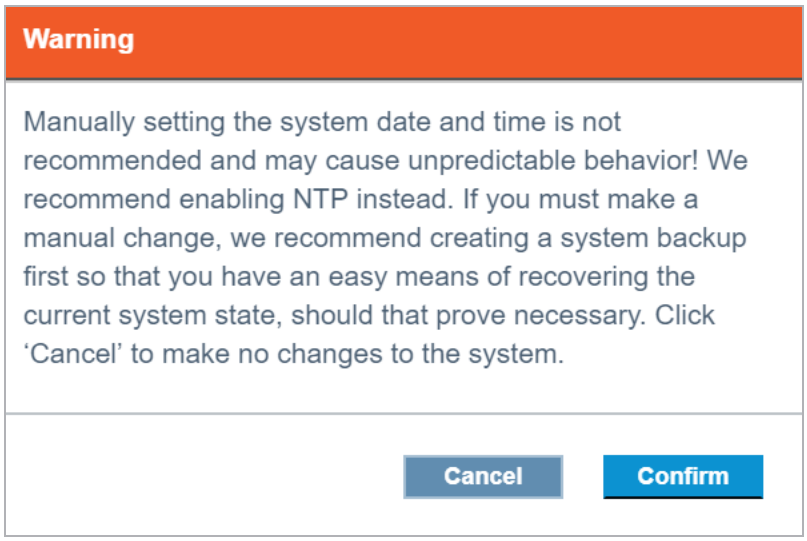
> You can have up to three NTP servers in the **Time Servers** field. You must list the NTP servers in order of preference and separate each one using a comma. You can specify a time server as an IP address, a fully qualified domain name (FQDN) or a public NTP server pool name. The time servers entered are validated on use, not when configured. If Kemp 360 Central cannot successfully contact the first time server, it tries the second time server (if specified); and, if that does not work, it tries the third time server (if specified). If all specified time servers cannot be contacted, then the warning described above is displayed in the banner.

Kemp 360 Central automatically displays the time zone of your local Kemp 360 Central session as determined by your browser. If you change your browser time zone setting, this is reflected on Kemp 360 Central. In the screenshot below, the system date and time is shown at the top of the display, along with the time zone (UTC-01:00) currently being used by the browser.



- In the example above, the time zone is changed to Atlantic/Azores on the local machine, however, Kemp 360 Central displays the system date and time and also the time relative to UTC. The local time zone used by the browser is used in the Kemp 360 Central UI to display most time and date information, including scheduled actions (like backups and firmware upgrades) and the graphical data displays on the Graphs tab. The log viewer, however, uses UTC time to display log entries to make it easier to coordinate times between log events.

To manually set the time, ensure the **Enable NTP** check box is clear, then set the date and time using the dropdown menus provided. If you try to change the time manually, the following warning appears:



> Do not change the time manually unless you are not using NTP. Kemp does not recommend manual date/time changes and recommends using NTP

You can authenticate the NTP server using a shared secret and key. To do this:

1. Select the **Authenticate** check box. This activates the **NTP Shared Secret** and **NTP Key ID** fields.
2. Select the **NTP Key Type** (at present, this is either MD5 or SHA-1).
3. Type the **NTP Shared Secret** string. This can be up to 40 characters in length. If it is more than 20 characters, it is treated as a hex string.

> The NTP Shared Secret must match the shared secret specified in the NTP time server's configuration, or authentication with the NTP server will fail and the time will not be synchronized. If you specify multiple time servers, they must all use the same NTP authentication parameters.

4. Type the **NTP Key ID**. This must be in the range from 1 to 65534.
5. Click **Apply** to apply the changes.

23 Storage

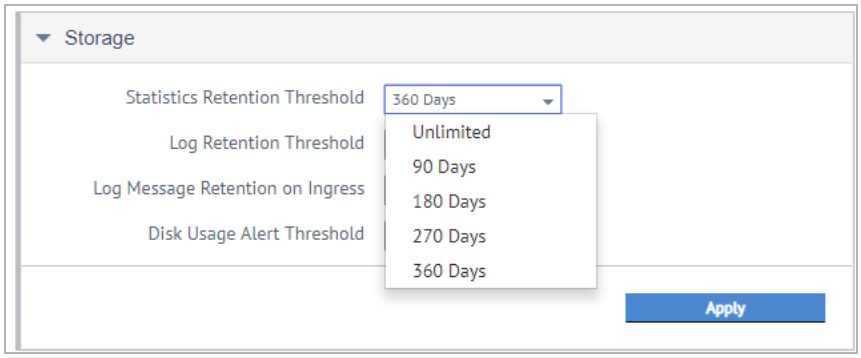
To ensure your installation of Kemp 360 Central remains functional, you can control how much data is retained using the **Storage** and **Device Log Management** features. To access, click **Settings and Configuration > Storage**. After you set a value, click **Apply** to apply the change.

Storage

There are four settings you can manage here:

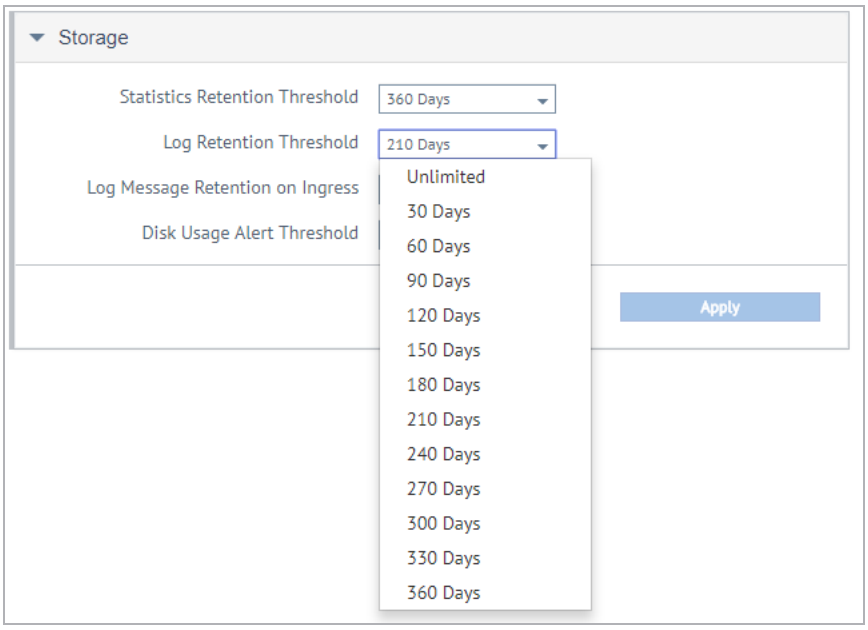
- **Statistics Retention Threshold** (default value is 90 Days)
- **Log Retention Threshold** (default value is 90 Days)
- **Log Message Retention on Ingress** (default value is Error)
- **Disk Usage Alert Threshold** (default value is 80%)

> The default values are for a new system. On upgrade, no changes are made to the existing settings for these controls. If you are upgrading from a system that does not support these controls, the retention thresholds are set to 'unlimited' to match the effective settings in older releases.



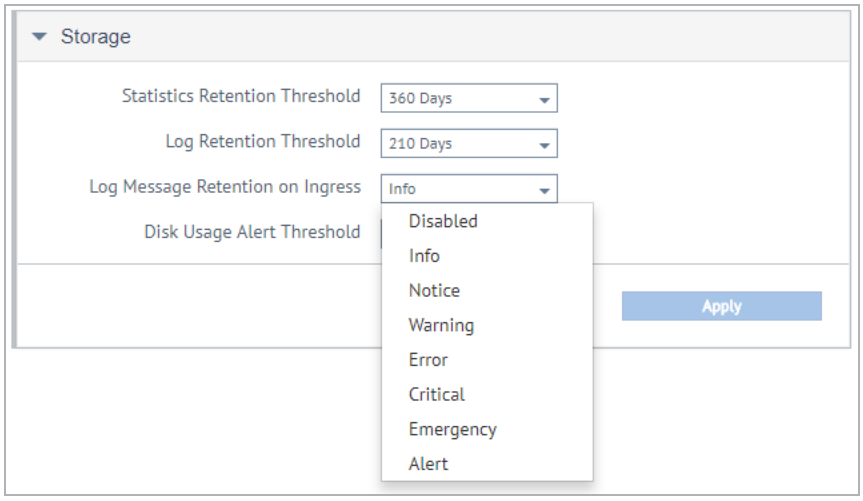
Statistics Retention Threshold

Here you can set the maximum number of days that managed device statistics data are retained. Any data above this threshold is deleted periodically. The available options are **Unlimited**, **90 Days**, **180 Days**, **270 Days**, and **360 Days**.



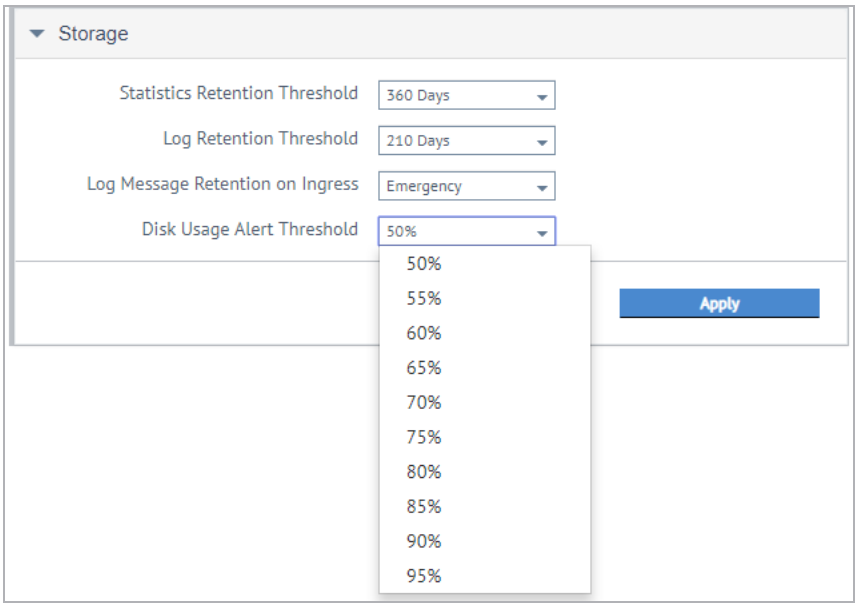
Log Retention Threshold

This is the maximum number of days that managed device log data are retained for. Any data above this threshold is deleted periodically. The available options range from **Unlimited** to **360 Days**.



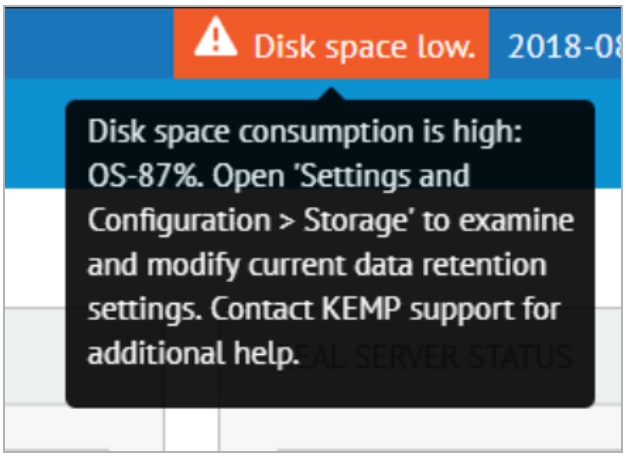
Log Message Retention on Ingress

This option refers to the lowest log message severity level accepted on receipt from a managed device. Any message received containing a lower severity level is dropped on receipt, regardless of the log level setting on the managed device. Besides **Disabled**, the range of options, from highest to lowest priority, is as follows: **Emergency**, **Alert**, **Critical**, **Error**, **Warning**, **Notice**, and **Info**.



Disk Usage Alert Threshold

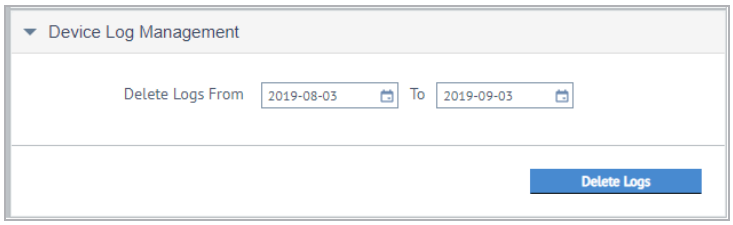
This option enables you to set the percentage of disk space at which the system begins sending storage alerts. The alerts are sent until the disk space usage falls below the specified percentage. The values range from **50%** to **95%**.



When the system reaches a disk alert threshold set by the user, an orange alert appears on the UI informing you about this (this is also stored in Syslog). When this happens, you could select a shorter **Statistics Retention Threshold** or **Log Retention Threshold** to free up space. If you do not, there is a critical disk alert threshold set by the system of 95%. If this threshold is reached, the system sends out another alert and stops collecting logs and statistics until you contact Support. An email notification alert is also sent to anyone who has their SMTP settings configured.

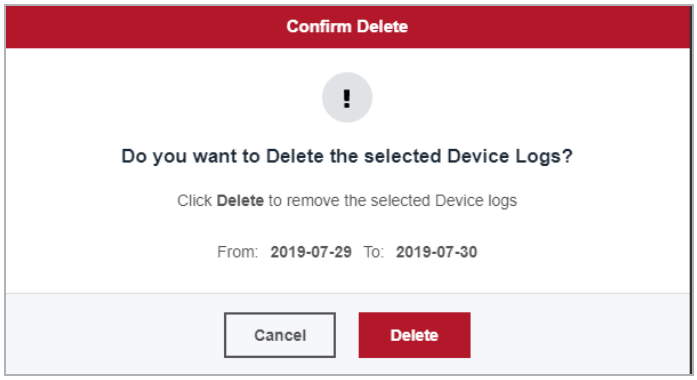
If you change the **Statistics Retention Threshold**, any data older than the set value will no longer be available for graphs or reporting.

Device Log Management



As an **admin** user, you can free up disk space by deleting log files that you no longer need. To do this, perform the following steps:

1. Expand the **Device Log Management** section.
2. Select the date range of the logs you want to delete in the **Delete Logs From** field.
3. Click **Delete Logs**.



4. If you want to delete the selected device logs, click **Delete**; if not, click **Cancel**. The applicable logs are removed and are no longer visible in the **Global Repository**.

If you are logged in as a non-admin account, you are not able to use this functionality.

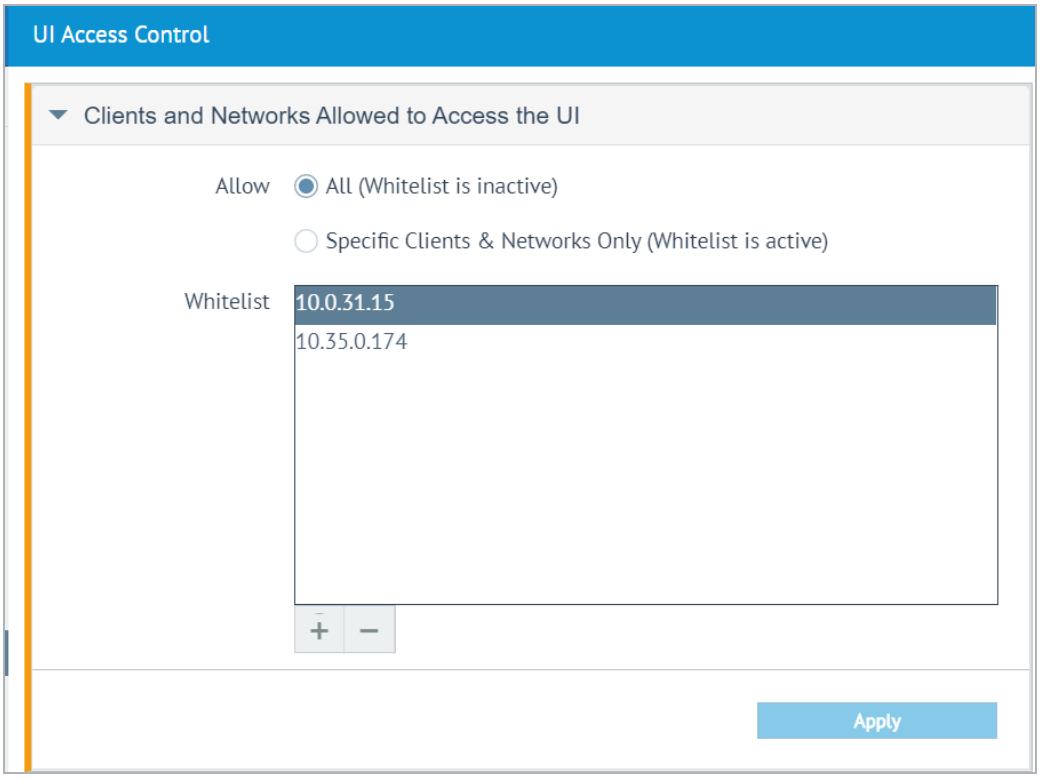
24 UI Access Control

To access **UI Access Control**, click **Settings and Configuration > UI Access Control**.

There are a number of actions you can perform as an **admin** user in this menu. These are:

- Control what clients and networks are allowed to access the UI
- Download the root certificate
- Identify the UI server certificate
- Upload the UI server certificate
- Select the UI TLS protocols

24.1 Clients and Networks Allowed to Access the UI



By default, Kemp 360 Central allows connections from any client network, however, you can create a whitelist where you can specify what networks you want UI access to be available on. If you try to

access a Kemp 360 Central machine from a network or IP address that is not on the whitelist, an error occurs and you are not allowed access to the system.

> 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. This is required to support API access from all managed devices.

By default, the **All (Whitelist is inactive)** option is selected. You can edit the whitelist when it is in either the inactive or active state. To add an entry to the whitelist, perform the following steps:

1. Click the plus icon.
2. Type the IP address of the network (or individual IP address) you want to add to the whitelist and click **Add**.

> You can add multiple IP addresses by separating each address with a comma. You can also type the IP address in CIDR format, for example, 192.168.100.0/24, to whitelist a range of IP addresses.

3. To remove an IP address from the whitelist, select the address and click the minus icon.

> As a lockout protection mechanism, the IP address of the device from where the UI is being accessed is always added to the whitelist, even if it is not specified by the user.

4. Click **Apply** to apply your changes.

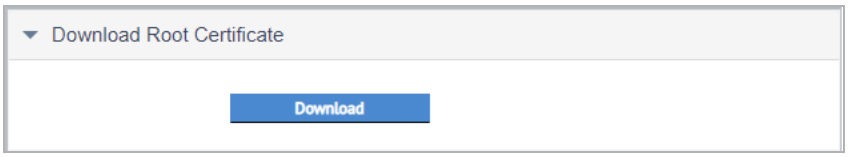
> If you are using a private IP address, that address is automatically added to the whitelist. The same applies for a public IP address.

After you have added all the IP addresses you need to the whitelist, you can then enable the whitelist by selecting the **Specific Clients & Networks Only (Whitelist is active)** option and clicking **Apply**.

24.2 User Interface SSL Certificate Management

The Kemp 360 Central User Interface (UI) is delivered with a default, self-signed SSL certificate to secure communication between the client browser and Kemp 360 Central. Because it is a self-signed certificate, it causes security warnings that the user needs to click through before seeing the Kemp 360 Central login prompt in their browser.

To remove these security warnings, download the root certificate from Kemp 360 Central and install it as a trusted root certificate in your browser, as described in this section.



To download the root certificate, perform the following steps:

1. Click **Download**.

2. Navigate to the area in your browser where certificates are managed. For example, in Chrome, perform the following steps:

    a) Click **Settings > Advanced > Manage certificates**.

    b) Click **Trusted Root Certification Authorities**.

    c) Click **Import**. This opens the **Certificate Import Wizard**.

    d) Click **Next**.

    e) Browse to the location where your certificate is downloaded to.

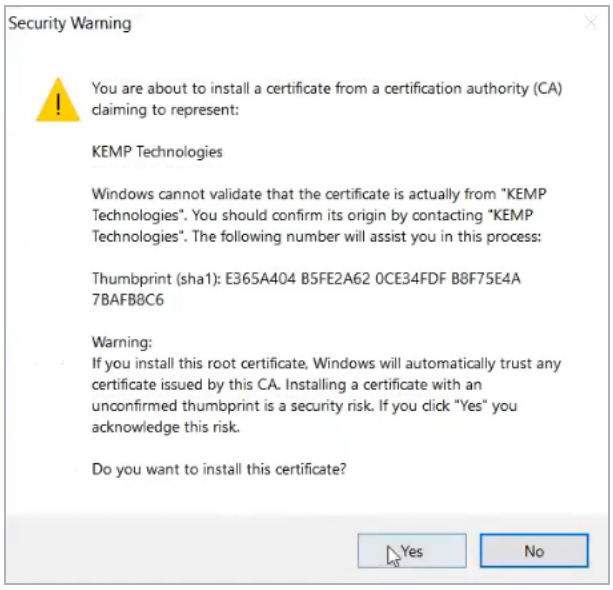
    f) Select **All Files** from the drop down list.

    g) Locate the certificate and select it.

    h) Click **Open**.

    i) Click **Next**.

    j) Click **Finish**.

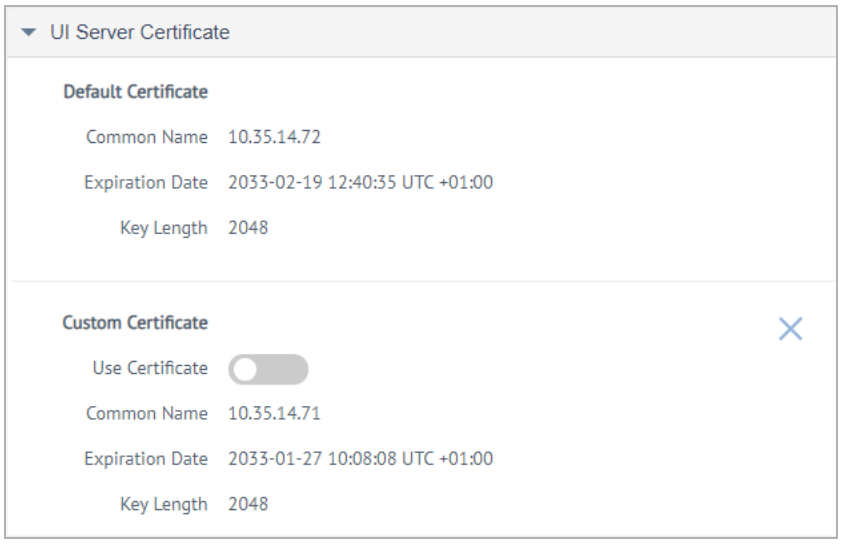


k) Click **Yes**.

The procedure may be different on different browsers.

When you return to Kemp 360 Central, you no longer see the screens relating to security exceptions.

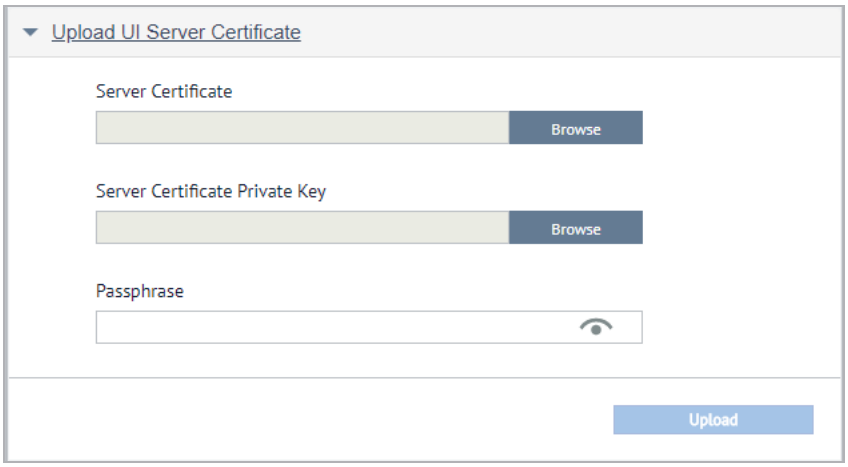
24.3 UI Server Certificate



In the **UI Server Certificate** section, you can view details about the default and custom certificate such as the **Common Name**, **Expiration Date**, and **Key Length**.

To use the custom certificate, click the **Use Certificate** button. To disable the **Custom Certificate**, click it again. To delete the certificate, first you must disable it.

24.4 Upload UI Server Certificate

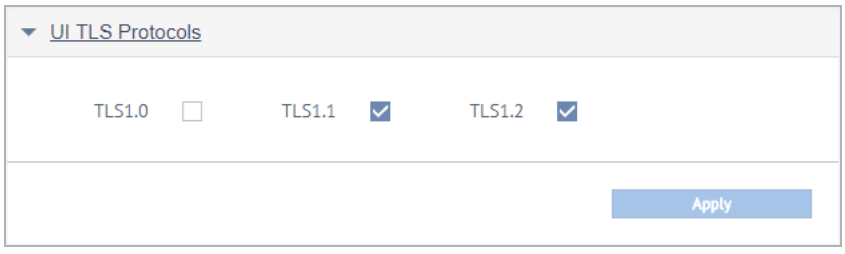


To upload a server certificate and or private key, browse to where the certificate or key is stored then click **Upload**.

> An error appears if you upload an invalid certificate or private key.

If a **Passphrase** is required, you must enter it in the field provided.

24.5 UI TLS Protocols



You can select the TLS protocols in this section. The options are TLS1.0, TLS1.1, and TLS1.2. Select the protocols you want and click **Apply**.

24.6 UI Supported SSL Ciphers

The following list of ciphers is supported by the UI:

- ECDHE-RSA-AES256-GCM-SHA384
- ECDHE-ECDSA-AES256-GCM-SHA384
- ECDHE-RSA-AES256-SHA384
- ECDHE-ECDSA-AES256-SHA384
- ECDHE-RSA-AES256-SHA
- ECDHE-ECDSA-AES256-SHA
- DHE-DSS-AES256-GCM-SHA384
- DHE-RSA-AES256-GCM-SHA384
- DHE-RSA-AES256-SHA256
- DHE-DSS-AES256-SHA256
- DHE-RSA-AES256-SHA
- DHE-DSS-AES256-SHA
- DHE-RSA-CAMELLIA256-SHA
- DHE-DSS-CAMELLIA256-SHA
- ECDH-RSA-AES256-GCM-SHA384
- ECDH-ECDSA-AES256-GCM-SHA384
- ECDH-RSA-AES256-SHA384
- ECDH-ECDSA-AES256-SHA384
- ECDH-RSA-AES256-SHA
- ECDH-ECDSA-AES256-SHA
- AES256-GCM-SHA384
- AES256-SHA256
- AES256-SHA

- CAMELLIA256-SHA
- ECDHE-RSA-AES128-GCM-SHA256
- ECDHE-ECDSA-AES128-GCM-SHA256
- ECDHE-RSA-AES128-SHA256
- ECDHE-ECDSA-AES128-SHA256
- ECDHE-RSA-AES128-SHA
- ECDHE-ECDSA-AES128-SHA
- DHE-DSS-AES128-GCM-SHA256
- DHE-RSA-AES128-GCM-SHA256
- DHE-RSA-AES128-SHA256
- DHE-DSS-AES128-SHA256
- DHE-RSA-AES128-SHA
- DHE-DSS-AES128-SHA
- DHE-RSA-CAMELLIA128-SHA
- DHE-DSS-CAMELLIA128-SHA
- ECDH-RSA-AES128-GCM-SHA256
- ECDH-ECDSA-AES128-GCM-SHA256
- ECDH-RSA-AES128-SHA256
- ECDH-ECDSA-AES128-SHA256
- ECDH-RSA-AES128-SHA
- ECDH-ECDSA-AES128-SHA
- AES128-GCM-SHA256
- AES128-SHA256
- AES128-SHA
- CAMELLIA128-SHA

25 Appendix: Password Information

You must adhere to the following rules when creating a password in the **User Management** section:

- Passwords must be a minimum of eight characters long and must contain at least one uppercase letter.
- Passwords must contain at least one number.
- All ASCII alphanumeric and printable special characters are supported.
- The bar below the password field changes color based on the strength of your password. Blue indicates a weak password, orange a stronger password, while green indicates the strongest level.

To improve the strength of the password, use special characters, capital letters and numbers. Making your password long also increases its strength.

26 References

Related documents are listed below:

Kemp 360 Central API, Interface Description

Kemp 360 Central for Azure, Installation Guide

Virtual Services and Templates, Feature Description

Web User Interface WUI, Configuration Guide

User Management, Feature Description

Health Checking, Feature Description

Last Updated Date

This document was last updated on 21 August 2020.