

KEMP 360

KEMP 360 Central Feature Description

VERSION: 17.0

UPDATED: MARCH 2017

Contents

1	Introduction	6
1.1	Document Purpose	7
1.2	Intended Audience.....	7
2	KEMP 360 Central Interface Description	8
2.1	Activation and Initial Login.....	8
2.2	Logging Out	10
2.3	Welcome Screen	11
2.4	About Screen.....	14
2.5	Help Screen	14
3	Global Dashboard.....	15
3.1	Device Overview	15
3.2	Infrastructure	17
3.3	Application Health	19
4	Network and Device Management	21
4.1	Network Management.....	23
4.1.1	Add a Network	23
4.1.2	Modify a Network	24
4.1.3	Remove a Network.....	24
4.2	Device Management	24
4.2.1	Adding Devices.....	25
4.2.2	Modify a Device	29
4.2.3	Remove a Device.....	30
4.2.4	Certificate-based LoadMaster Authentication	30
5	System Configuration.....	31
5.1	Open the LoadMaster UI from KEMP 360 Central.....	31
5.2	LoadMaster Reboot	31
5.2.1	Schedule a LoadMaster Reboot	32
5.3	Template Management	33
5.3.1	Upload the Template to KEMP 360 Central Global Repository	34

5.3.2	Upload a Template File to a LoadMaster	34
5.4	Update the LoadMaster Firmware.....	35
5.4.1	Upload the LoadMaster Firmware Update File to the Global Repository	35
5.4.2	Update the Firmware on Selected LoadMasters	36
5.4.3	Schedule a LoadMaster Firmware Update.....	37
5.5	Backup/Restore.....	38
5.5.1	Back Up a LoadMaster using KEMP 360 Central.....	38
5.5.2	Importing a LoadMaster Backup into KEMP 360 Central	39
5.5.3	Restore LoadMaster Settings.....	40
5.5.4	Schedule a LoadMaster Backup/Restore	41
5.5.5	Backup and Restore KEMP 360 Central	42
5.5.6	Restoring KEMP 360 Central ASL Notes.....	44
5.5.7	Configuring Syslog Collection from Managed Devices.....	44
5.5.8	LoadMaster Syslog Collection	44
5.6	HA Configuration.....	46
6	Service Configuration.....	50
6.1	Virtual Service Management	50
6.1.1	Display the List of Virtual Services Attached to a LoadMaster	50
6.1.2	Add a Virtual Service	50
6.1.3	Modify a Virtual Service	51
6.1.4	Remove a Virtual Service	52
6.1.5	Migrate a Virtual Service.....	52
6.2	SubVS Management.....	53
6.2.1	Display a List of SubVSs on a Virtual Service.....	53
6.2.2	Add a SubVS	53
6.2.3	Modify a SubVS	54
6.2.4	Delete a SubVS.....	55
6.3	Real Server Management.....	55
6.3.1	Display a List of Real Servers on a Virtual Service.....	55
6.3.2	Add a Real Server	56
6.3.3	Modify a Real Server	57

6.3.4	Remove a Real Server	57
6.3.5	Health Check	57
7	Monitoring	59
7.1	Network and Device Health	59
7.2	System Statistics.....	64
7.3	Global Repository.....	65
7.4	Logging	65
7.4.1	Source	66
7.4.2	Filter	67
7.4.3	Log Search Results.....	69
8	Access Control.....	70
8.1	User Management	70
8.2	Group Management.....	71
8.2.1	Group Details	72
8.2.2	Group Members.....	73
8.2.3	Group Resources.....	74
9	KEMP 360 Central System Administration.....	75
9.1	Reboot/Shutdown KEMP 360 Central.....	75
9.2	SMTP Settings	76
9.3	Enable Temporary SSH Access for Diagnostic Purposes	77
9.4	Proxy Settings.....	78
10	License Management.....	79
11	Firmware Management	80
11.1	Update the KEMP 360 Central Firmware - Online Method	80
11.2	Update the KEMP 360 Central Firmware – Offline Method	81
12	Metered Licensing Management.....	83
12.1	Instances	83
12.2	Report Data.....	83
13	Scheduled Actions.....	87
13.1	View Scheduled Actions.....	87
13.2	Modify Scheduled Actions	87

13.3	Delete a Scheduled Action	88
14	Log Files.....	90
14.1	System Logs.....	90
14.2	Diagnostic Logs.....	90
14.3	Log Settings	91
15	Appendix: Password Information	92
	References	93
	Document History	94

1 Introduction

KEMP 360 Central is a centralized management, orchestration, and monitoring application that enables the administration of deployed LoadMaster and select third party Application Delivery Controllers (ADC).

KEMP 360 Central provides the ability to perform administrative tasks on each or all of the attached devices. This provides ease of administration because multiple devices can be administered in one place, rather than accessing each individually.

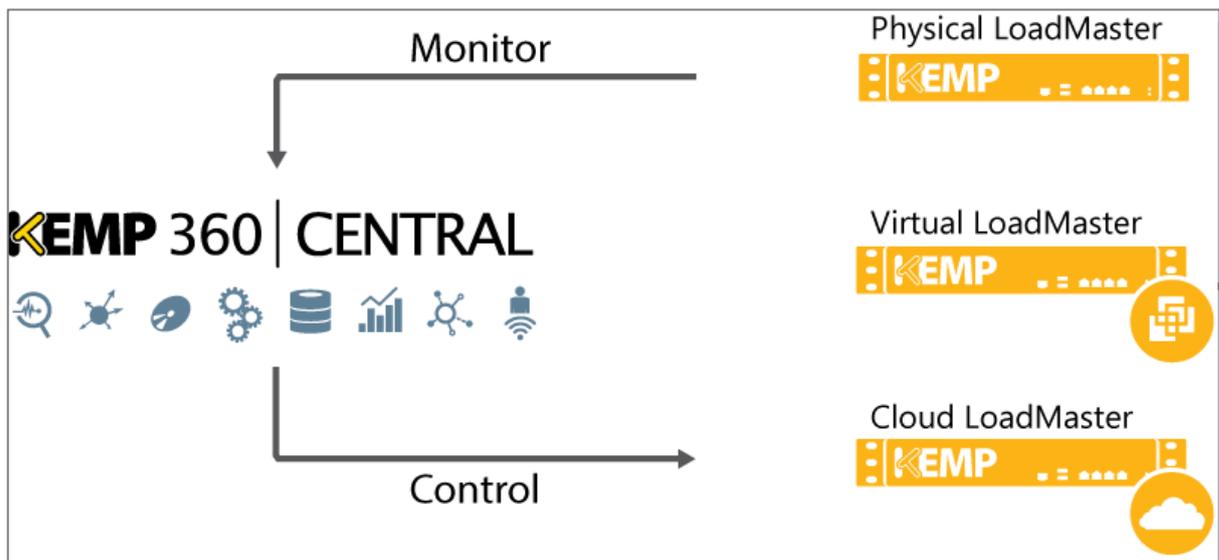


Figure 1-1: KEMP 360 Central Network Architecture

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

- Monitor performance and usage statistics of the networks, sub-networks, and LoadMasters (including any Virtual Services, Real Servers and SubVSs), which are attached
- Add/remove and monitor third party products such as AWS ELB, HAProxy, NGINX and F5 BIG-IP.
- View a list of available Virtual Services at both network and LoadMaster level
- View a list of available Real Servers at both a network and LoadMaster level
- View a list of available SubVSs at both network and LoadMaster level
- License LoadMasters locally using KEMP 360 Central with the Activation Server functionality
- License the KEMP 360 Central using offline, closed network licensing
- Allow KEMP 360 Central to access the Internet using a HTTP(S) proxy
- Reboot a LoadMaster, or reboot multiple LoadMasters simultaneously
- Upload application templates to KEMP 360 Central and deploy them to LoadMasters as needed
- Upload LoadMaster firmware packages to KEMP 360 Central and update and deploy LoadMaster firmware as needed

- Upload and perform offline, closed network firmware updates for KEMP 360 Central
- Store backups of LoadMaster settings and restore them to LoadMasters as needed
- Automatically configure syslog options in one or multiple LoadMasters
- View and filter LoadMaster syslogs
- Download diagnostic logs such as audit, debug and system logs
- Configure SMTP settings to allow KEMP 360 Central to send emails regarding critical errors

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 is for anyone interested in finding out more about KEMP 360 Central.

2 KEMP 360 Central Interface Description

This section of the document describes the screens available to users within KEMP 360 Central.

2.1 Activation and Initial Login

1. To access the KEMP 360 Central UI, in your browser, enter the IP address of the instance. A license activation screen appears.

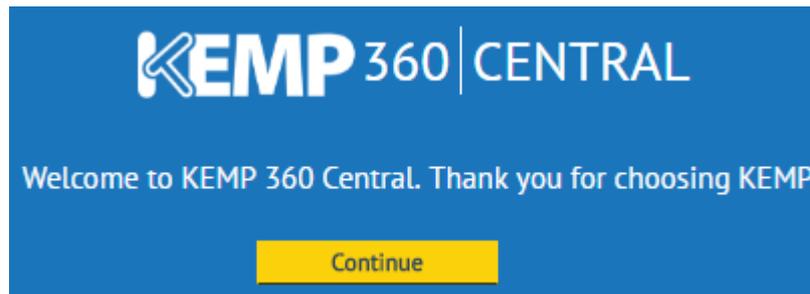


Figure 2-1: Initial Activation Screen

2. Click **Continue**.



Figure 2-2: Accept the License Agreement

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



Figure 2-2: Enter Credentials

4. If using the **Online** method, fill out the fields and click **License Now**.

An **Order ID** is supplied by KEMP when you purchase a KEMP 360 Central instance. Entering an **Order ID** is optional for standard licenses.

If using the **Offline** method, select **Offline**, obtain the license text, paste it into the field provided and click License Now.

If using manual licensing, provide the **Fingerprint** to a KEMP representative and enter the license string which they provide.

For detailed instructions on how to register for a KEMP ID and license the LoadMaster, refer to the **KEMP 360 Central Licensing, Feature Description**.

5. Enter your KEMP ID (the email address used when registering the KEMP account).

The **Order ID** is optional for standard licenses.

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. For step-by-step instructions on how to register for a KEMP ID, and for information on licensing in general, refer to the **KEMP 360 Central Licensing, Feature Description**.

6. Type your **Password**.

If you wish to display the password while entering it, click the eye icon.

7. Click **License Now**.

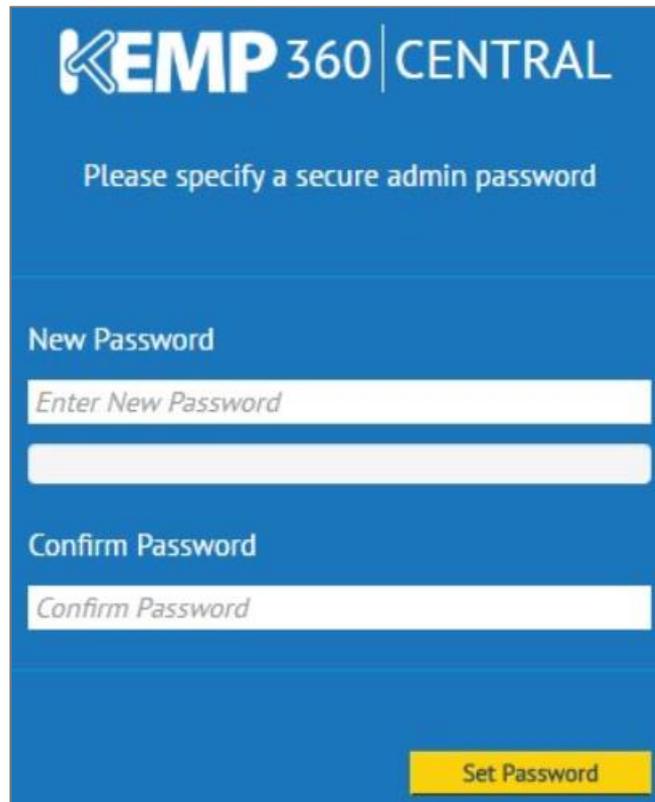


Figure 2-3: Set Admin Password

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

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.

Users may log in to KEMP 360 Central as either the **admin** user.

An **admin** has access to the full range of options in KEMP 360 Central.

2.2 Logging Out

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



Figure 2-4: Logout Button

2.3 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 a device for the first time 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.

Welcome to KEMP 360 Central

Add LoadMasters and optionally set administrative parameters using LoadMaster settings. [Skip this step](#)

1 Please provide the IP address and administrative login credentials needed to log in to a LoadMaster and click Add Device. The administrative and network settings from this LoadMaster will be used to configure settings.

▼ Add a Device

Device Type

IP Address : Port :

Username

Password

Collect Logs

Nickname

2 To notify you via email about important events. Please provide the address and credentials for an SMTP service.

▼ Set Up SMTP Settings

Email Address List

SMTP Host : Port :

SMTP Host User

SMTP Host Password

Connection Security

"From" Email

Figure 2-5: Welcome to KEMP 360 Central screen

When you have no devices configured, you can click **Skip this step** at the top right of the screen to continue without adding your LoadMaster. When you have one device set up, this button changes to **I've completed my setup**.

Only LoadMasters can be added to KEMP 360 Central using the **Welcome** screen. If you want to add another supported device type (such as F5 or NGINX), click the **Network and Device Administration** icon and then click the **plus** icon at the bottom left of the screen.

By default, the **Collect Logs** check box is enabled so that the LoadMaster sends logs to KEMP 360 Central automatically. Disabling this box means that you can still add the LoadMaster to KEMP 360 Central, but KEMP 360 Central will not have any information to display in the log widget on the dashboard or in the log viewer for that LoadMaster.

After you click **Add Device**, KEMP 360 Central looks at the configuration of the LoadMaster you added. If it contains SMTP configuration settings, KEMP 360 Central pre-populates the SMTP settings on KEMP 360 Central using the LoadMaster settings. If KEMP 360 Central is already configured for SMTP, you can choose to replace the current SMTP settings with the settings from the newly added LoadMaster.

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**.

Welcome to KEMP 360 Central

Add LoadMasters and optionally set administrative parameters using LoadMaster settings. I've completed my setup

1 Please provide the IP address and administrative login credentials needed to log in to a LoadMaster and click Add Device. The administrative and network settings from this LoadMaster will be used to configure settings.

▼ Add a Device

Device Type

IP Address : Port :

Username

Password

Collect Logs

Nickname

Add Device

2 To notify you via email about important events. Please provide the address and credentials for an SMTP service.

▼ Set Up SMTP Settings

Email Address List Send Test Email

SMTP Host : Port :

SMTP Host User

SMTP Host Password

Connection Security

"From" Email

Delete SMTP Settings
Apply

Figure 2-6: SMTP Settings prepopulated

The SMTP Setting pane is pre-populated from the LoadMaster if there are currently no SMTP settings on KEMP 360 Central. Note that not all fields are pre-populated. You must type the **SMTP Host User** and **SMTP Host Password** fields. In addition, you must also complete the **'From' Email** field.

From the KEMP 360 Central welcome page, you can perform several tasks.

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 (**Section 9.2**)
- Add a device (**Section 4.2**)

2.4 About Screen

Clicking the question mark button on the bottom-left of the UI brings users to the KEMP 360 Central **About** 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

2.5 Help Screen

The help screen provides a link to the KEMP documentation page and the KEMP Customer Support site.

3 Global Dashboard

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**.

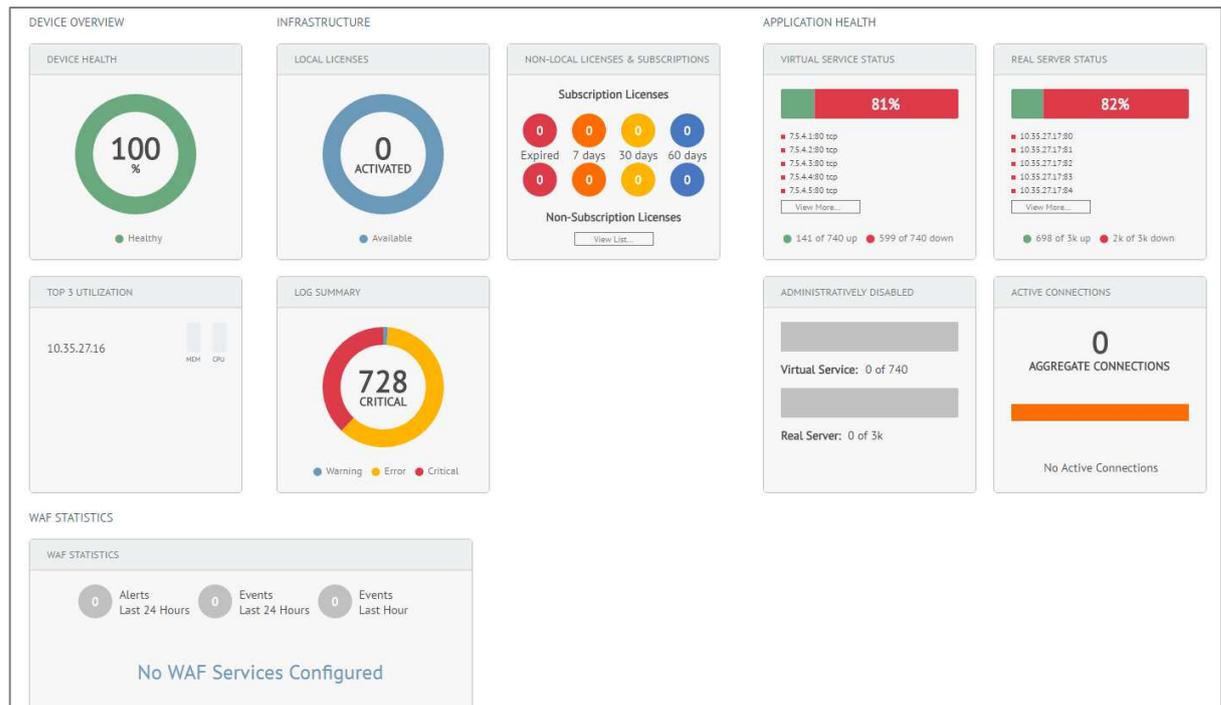


Figure 3-1: Global Dashboard

3.1 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.

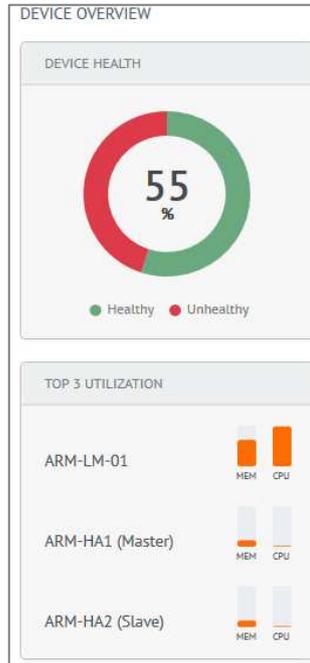


Figure 3-2: Device Overview Panel

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.

The health status of an unknown device is not checked.

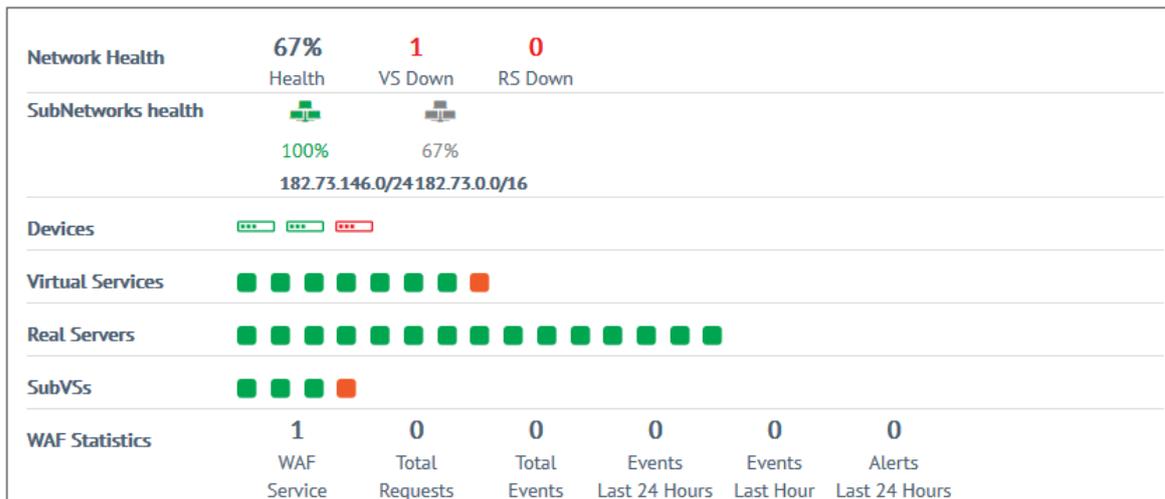


Figure 3-3: Detailed View of Device Health

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.

3.2 Infrastructure

The Infrastructure section contains three panels, **Local Licenses** (Activation Server Local, ASL, licenses), **Log Summary** and **Non-Local Licenses & Subscriptions**. If you hover over the **Local Licenses** panel, you can see how many licenses are activated. If you click the **Local Licenses** panel, the **Metered Licensing Management** screen opens. Here you can view information on instances and report data. See **Metered Licensing Management** for more information.

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



Figure 3-4: Infrastructure Panel

In the **Non-Local Licenses & Subscriptions** panel you can quickly identify LoadMasters that are approaching or have passed an expiration date. The Non-Local Licenses & Subscriptions panel displays the number of Subscription and Non-Subscription licenses and these are color coded as follows:

- Red: Expired
- Orange: 7 Days
- Yellow: 30 Days

- Blue: 60 Days

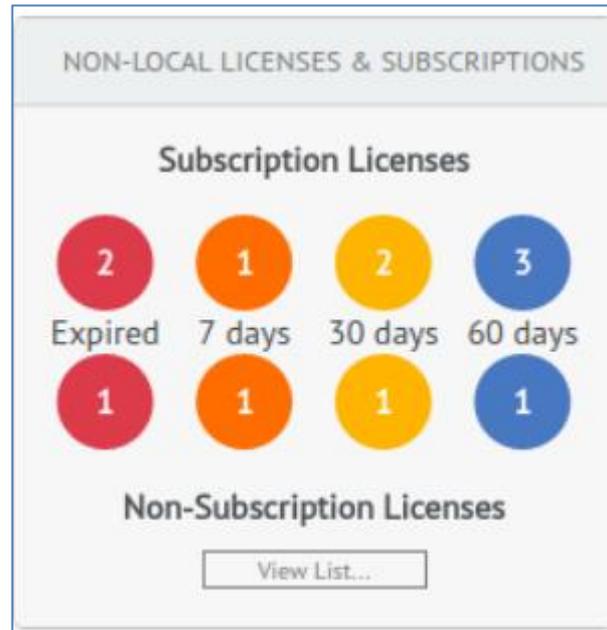


Figure 3-5: Non-Local Licenses & Subscriptions Widget

This feature does not include licenses activated by the KEMP 360 Central Activation Server Local (ASL) feature; these are reported in a separate dashboard widget.

You will receive an alert on the Non-Local Licenses & Subscriptions widget when a subscription expiration has occurred (or is about to occur within 7, 30 or 60 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 Non-Local Licenses & Subscriptions widget, you can view the Licenses table, which provides information on the type of license and the expiration date.

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

System Administration

- ▶ System Reboot
- ▶ Templates
- ▶ Update LoadMaster Firmware
- ▶ Backup/Restore
- ▼ Licenses

IP Address	Nickname	License or Subscription	Expiration Date
10.35.26.22		Classic	2018-02-14 05:00

3.3 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.

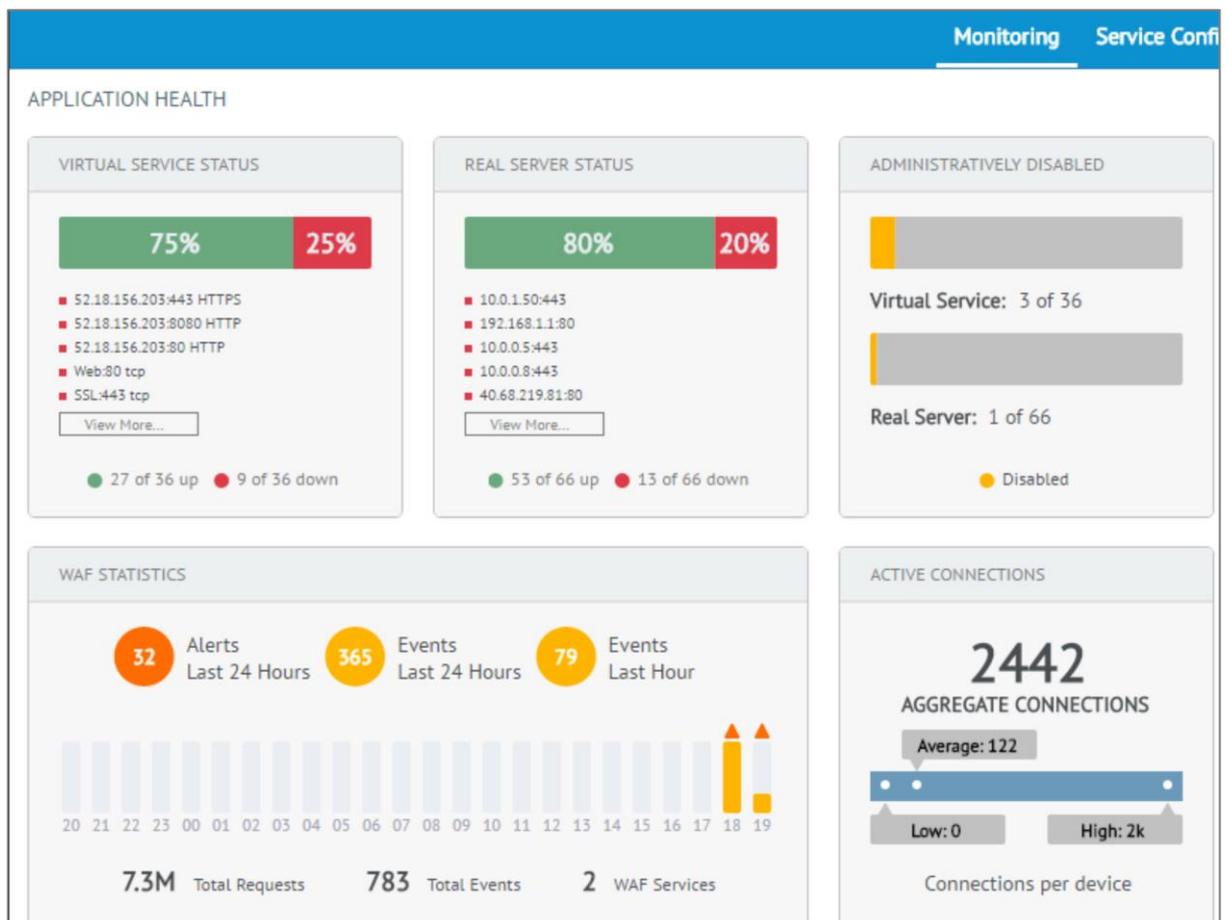


Figure 3-6: Application Health Panel

- **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, red indicates it is down and grey indicates it is administratively disabled. 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.
- **WAF Statistics** – This panel displays the following:
 - The number of configured WAF services
 - The total number of requests recorded
 - The total number of events recorded
 - 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
 - The highest number of active connections recorded for a single device
 - The average number of active connections across all managed devices

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

Note that it can take some time for the Active Connections widget to update.

4 Network and Device Management



Table 4-4-1: System Configuration

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.

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).

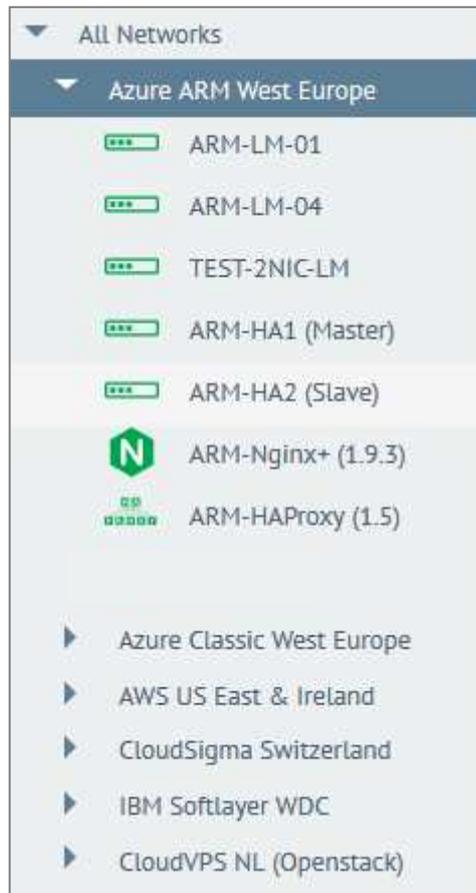


Figure 4-4-1: Networks

When in the **System Configuration** section - on the left-hand side of the KEMP 360 Central UI there is a networks area 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.

LoadMaster status is represented by the following icons:

Icon	Status
	LoadMaster is available/accessible and was not licensed using ASL
	LoadMaster is available/accessible and was licensed using ASL
	Certificate-based authentication to the LoadMaster has been broken. Please reenter the LoadMaster username and password. For further information, refer to Section 4.2.4 .
	LoadMaster has been licensed using ASL but the LoadMaster needs to be activated in KEMP 360 Central. Refer to the KEMP 360 Central Activation Server, Feature Description for further information.
	LoadMaster is rebooting (spinning)
	LoadMaster is not available/inaccessible

Table 4-4-2: LoadMaster Status

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
	Amazon Web Services (AWS) Elastic Load Balancer (ELB) device is available/accessible
	AWS ELB device is not available or it is inaccessible

Icon	Status
	F5 BIG-IP device is not available or is inaccessible
	F5 BIG-IP device is available/accessible
	Device is rebooting (spinning)

Table 4-4-3: Third Party Device Status

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.

4.1 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**.

4.1.1 Add a Network

1. Click the cloud icon on the left.

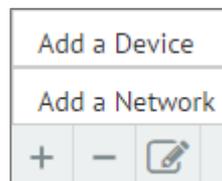


Figure 4-4-2: Add a Network

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

Add a Network

Parent Network

Network Address

Nickname

Figure 4-4-3: Network Details

3. If creating a top-level network, users should select **No Parent** from the **Parent Network** drop-down list.
6. If this is the first time adding a network using the KEMP 360 Central instance, the **Parent Node** drop-down list does not appear.

7. If adding a subnet, select a parent network from the **Parent Network** drop-down list.
8. Enter a recognisable **Nickname** for the network.
9. If no **Nickname** is entered here the Network's IP address will be displayed everywhere that the **Nickname** would have been shown.
10. Enter the IP address and CIDR in the **Network Address** box. The CIDR has a range from 1 to 31.
11. Click **Apply**. A message appears saying the network is added.

4.1.2 Modify a Network



Figure 4-4-4: Modify

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.

4.1.3 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.

4.2 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, which 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.

4.2.1 Adding Devices

This section shows users how to add devices to KEMP 360 Central. Currently supported devices are: KEMP LoadMasters, NGINX, HAProxy, AWS ELB and F5 BIG-IP.

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. For further information on LoadMaster licensing, refer to the **KEMP 360 Central Licensing, Feature Description**.
- Using a locally provisioned KEMP 360 Central Activation Server

KEMP 360 Central's optional Activation Server functionality allows you license client LoadMasters locally without needing to contact the KEMP license server. When activating a LoadMaster in this way, the LoadMaster automatically gets added to KEMP 360 Central. For more information on the Activation Server feature (including configuration), refer to the **KEMP 360 Central Activation Server, Feature Description**.

This section assumes that the Activation Server functionality is not being used.

Before a device can be added to KEMP 360 Central, a network must exist. For steps on how to add a network, refer to **Section 4.1**.



Figure 4-4-5: Cloud Icon

1. Click the cloud icon on the left.



Figure 4-4-6: Select the network

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).

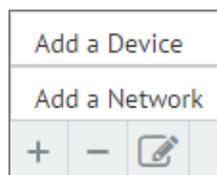
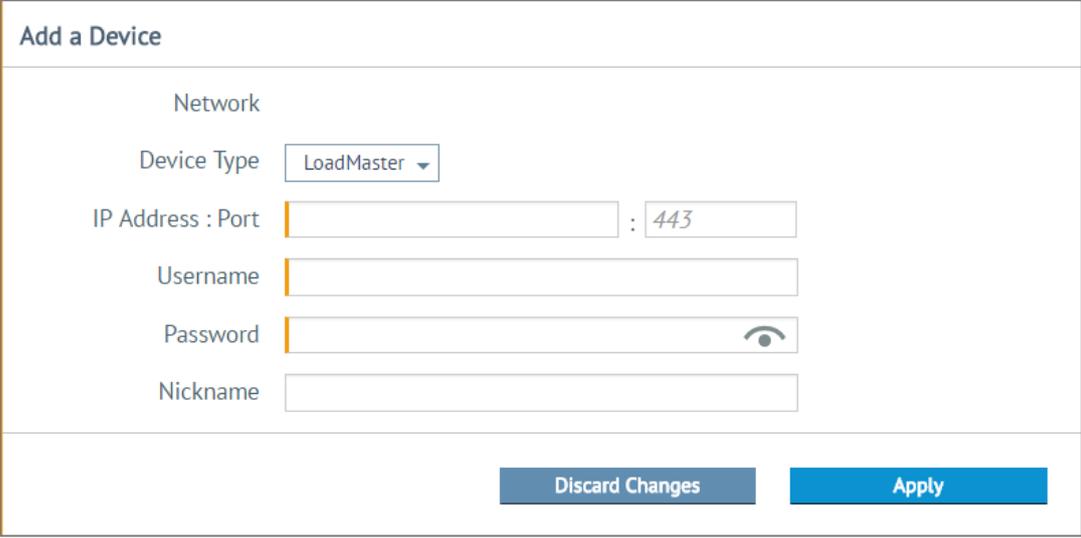


Figure 4-4-7: Add a LoadMaster

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

4.2.1.1 Add Details for a LoadMaster



Add a Device

Network

Device Type

IP Address : Port :

Username

Password

Nickname

Figure 4-4-8: LoadMaster Details

Use the following steps when adding the details for a LoadMaster only:

1. From the **Device Type** drop-down list, select **LoadMaster**.
2. Type the **IP Address** of the LoadMaster.

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

3. Enter the **Port** number.
4. In an Azure environment, type **8443** as the **Port**.

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

5. Type the **Username** and **Password** of the LoadMaster.
6. Type the **Alternate WUI Access** address for LoadMasters licensed using ASL. 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.

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

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

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

4.2.1.2 Add Details for a Third Party Device

In addition to LoadMasters, KEMP 360 Central gives users the ability 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:

Figure 4-4-9: Add a Third Party Device

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.

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.	✓	✓		

Field	Description	NGINX	HAProxy	AWS-ELB	F5-BIGIP-LTM
Access Key ID	Required. The 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			✓	
Public Address	Required only for Azure and ASL, otherwise optional. Specify the FQDN returned by DNS for the device type or specify the IP address followed by a colon and port number (for example, 10.10.10.10:443).	✓	✓	✓	✓
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.	✓	✓	✓	✓

Table 4-4: Fields available for different Device Types

4.2.1.3 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 organise 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).

4.2.2 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.

The screenshot shows the 'Edit LoadMaster' configuration form. It includes the following fields and values:

- Network:** A dropdown menu showing 'All Networks - 0.0.0.0/0'.
- IP Address : Port:** Two input fields containing '23.97.129.165' and '8443'.
- Username:** An empty text input field.
- Password:** An empty text input field.
- Alternate WUI Access:** Two input fields, the second containing '443'.
- Nickname:** An empty text input field.

At the bottom of the form are two buttons: 'Discard Changes' (grey) and 'Apply' (blue).

If your initial connection fails and you need to use an alternate address to access the WUI, 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 **Section 4.2.4**.

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.

4.2.3 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.

4.2.4 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 will be 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.

When certificate-based authentication is enabled and working, it will not be possible to edit the LoadMaster username and password on KEMP 360 Central. If any of the requirements for certificate-based authentication are not met, for example if Session Management becomes disabled on the LoadMaster – the authentication will break and the LoadMaster credentials will need to be re-entered into KEMP 360 Central to re-establish the connection. For further information on certificate-based authentication in general, refer to the **User Management, Feature Description**.

5 System Configuration



Figure 5-1: LoadMaster 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.

5.1 Open the LoadMaster UI from KEMP 360 Central

Clicking the Open WUI 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:

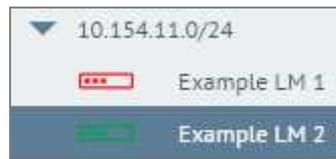


Figure 5-2: Select LoadMaster

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

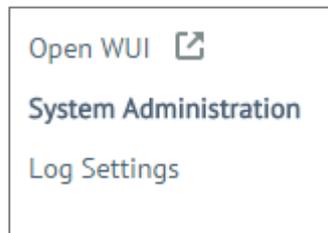


Figure 5-3: Open WUI

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

5.2 LoadMaster Reboot

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

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.



Figure 5-4: Reboot a LoadMaster

- To reboot a single LoadMaster, select the check box beside the LoadMaster for rebooting and click the **Reboot** button.
- Reboot multiple LoadMasters by ticking the checkbox of each LoadMaster and then clicking the **Reboot Selected** button. Alternatively, choose the **Select All** checkbox and click the **Reboot All** button to reboot all LoadMasters in the relevant network.



Figure 5-5: Rebooting

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

5.2.1 Schedule a LoadMaster Reboot

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

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

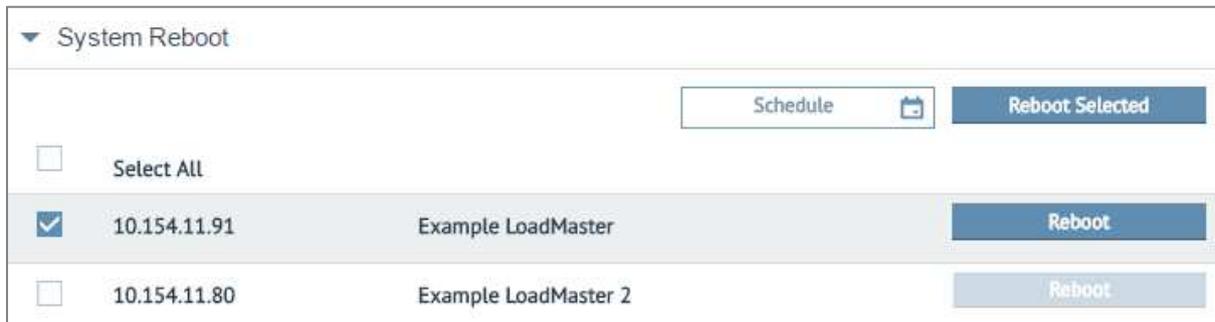


Figure 5-6: System Reboot Screen

- Expand the **System Reboot** section.
- 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, select the **Select All** check box.

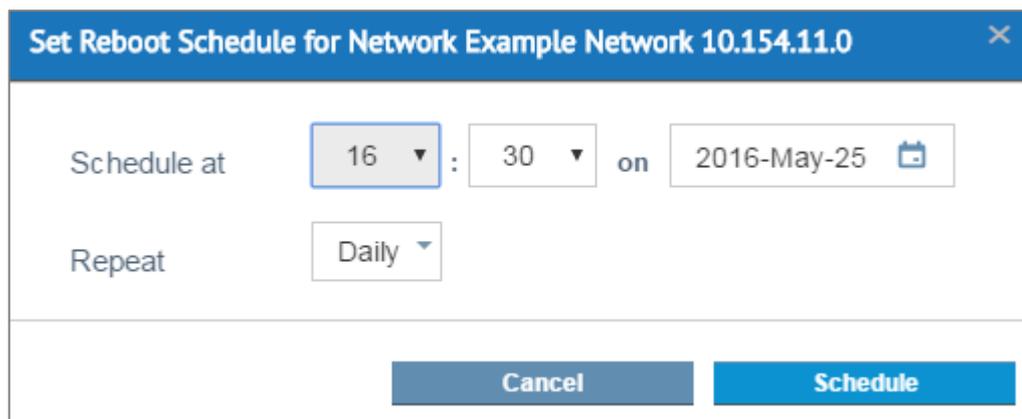


Figure 5-7: Schedule Screen

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

Tasks cannot be scheduled within one hour of each other.

- Click **Schedule**.
Further information on scheduling can be found in Scheduled Actions.

5.3 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.

5.3.1 Upload the Template to KEMP 360 Central Global Repository

To do this, use the following steps:



Figure 5-8: Global Repository

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

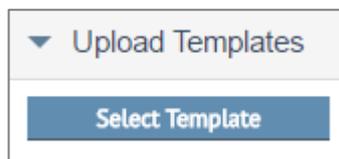


Figure 5-9: Select Templates

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

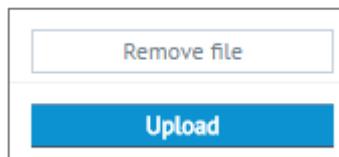


Figure 5-10: Upload

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

5.3.2 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.

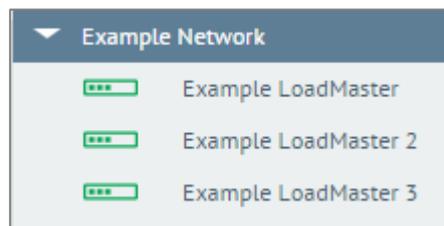


Figure 5-11: Select the Network/LoadMaster

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

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



Figure 5-12: Select Template

If you selected a network instead of a LoadMaster, you can tick multiple LoadMasters and install a template on them all at one time.

- From the **Select a template to apply** drop-down menu, click the template you wish to add.
- Do one of the following:
 - If you selected a single LoadMaster in **Step 3**, click Upload Selected to install the template on that LoadMaster.
 - If you selected a network in **Step 3**, tick the LoadMasters on which you want to install the template, and then click **Upload Template**.
- A message will appear when the upload completes.

5.4 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.

5.4.1 Upload the LoadMaster Firmware Update File to the Global Repository

To do this, follow the steps below:



Figure 5-13: Global Repository Icon

- In the menu, click the **Global Repository** icon and then click **Firmware Management**.

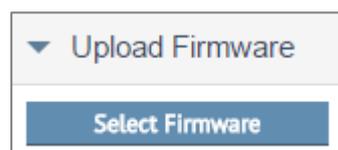


Figure 5-14: Upload LoadMaster Firmware

- Click **Select Firmware**.

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.

5.4.2 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. 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.

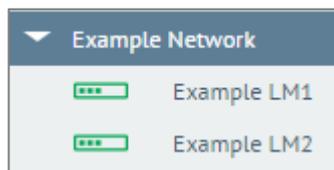


Figure 5-15: Select network/LoadMaster

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.



Figure 5-16: Update LoadMaster Firmware

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 Selected/Update All** 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. Wait for the firmware update to complete.

When the update is finished, the LoadMaster automatically reboots.

When the firmware update is complete and the LoadMaster(s) successfully rebooted, the LoadMasters come back online and KEMP 360 Central reflects the LoadMaster status.

5.4.3 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 **Section 5.4.1**.
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.

Update LoadMaster Firmware			
Select a firmware to apply		Schedule	Update Selected
<input type="checkbox"/>	Select All		
<input type="checkbox"/>	10.154.11.91	Example LoadMaster	unknown
<input type="checkbox"/>	10.154.11.80	Example LoadMaster 2	unknown

Figure 5-17: Firmware Update Screen

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.

Set Update Firmware Schedule for Network Example Network 10.154.11.0 ✕

Schedule at : on

Repeat

Figure 5-18: Schedule Screen

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 **Section 13**.

5.5 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 **Section 5.5.1** 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 **Section 5.5.2** for steps on how to do this.

5.5.1 Back Up a LoadMaster using KEMP 360 Central

LoadMasters which exist in KEMP 360 Central may be backed up in the following way:

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

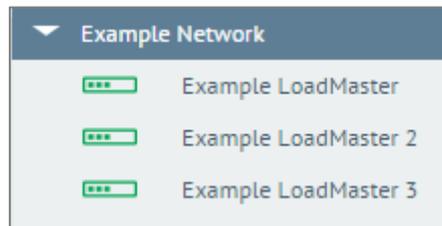


Figure 5-19: Select the Network/LoadMaster

2. Select the relevant Network/LoadMaster.
3. Select the **System Configuration** tab.
4. Expand the **Backup/Restore** section.



Figure 5-20: Backup a Single LoadMaster

5. If you selected a network, tick the LoadMasters which you would like to back up.

6. Click **Backup/Backup Selected**. A pop-up message displays saying the backup was created.

Once created, the backup file can be found in the **Backup Repository** section of the **Global Repository**.

5.5.2 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.

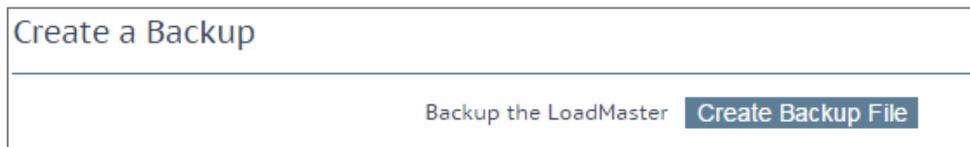


Figure 5-21: LoadMaster UI

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**.

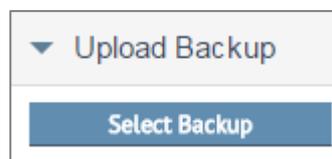


Figure 5-22: Upload Backup to KEMP 360 Central

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

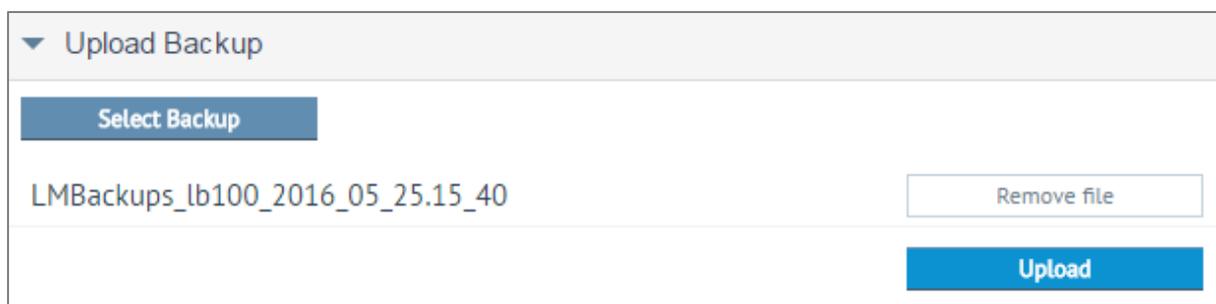


Figure 5-23: Upload

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 **Section 5.5.3**.

5.5.3 Restore LoadMaster Settings

When a backup file is available in KEMP 360 Central, the settings can be restored to a LoadMaster. To do this, perform the following steps:

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

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

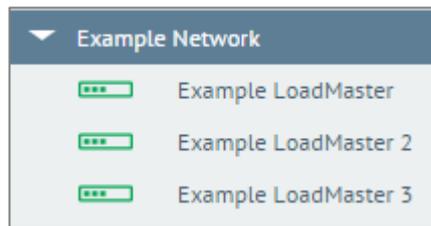


Figure 5-24: Select LoadMaster

2. Select the relevant network or LoadMaster.
3. Select the **System Configuration** tab.
4. Expand the **Backup/Restore** section.

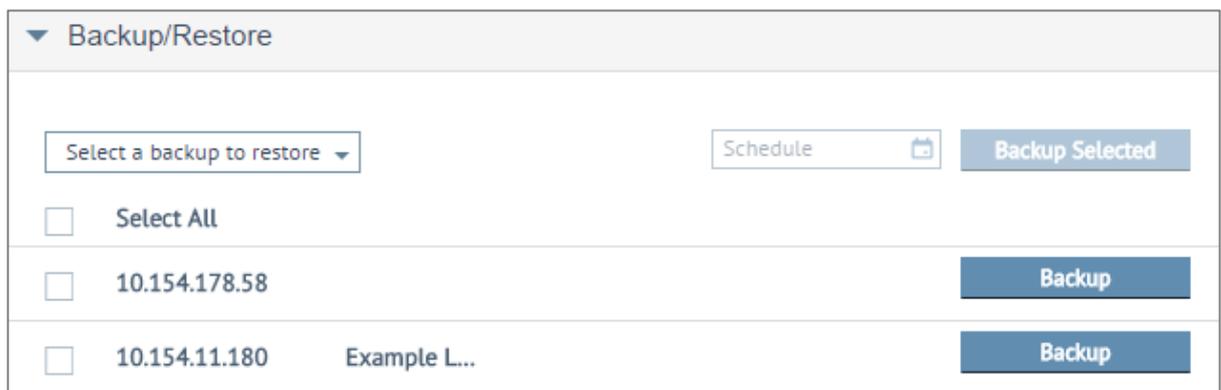


Figure 5-25: Select a Backup

5. If the network was selected, select the check boxes of the relevant LoadMaster(s).
6. Click the **Select a backup to restore** button and select the desired backup file.

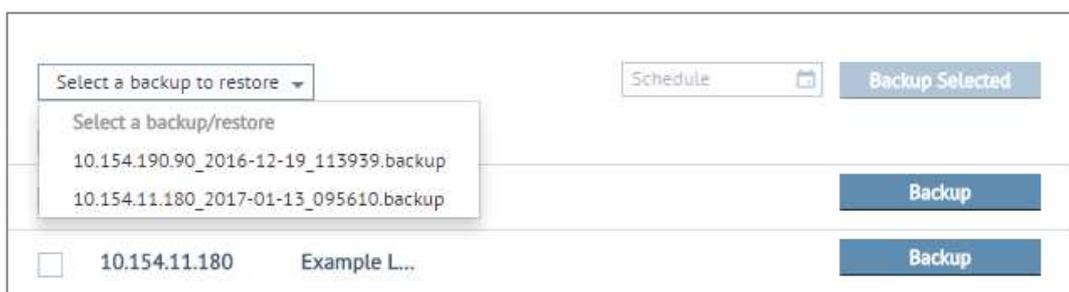


Figure 5-26: Restore Selected

7. Click the **Restore Selected** button.

8. A message will appear when the restore completes.

5.5.4 Schedule a LoadMaster Backup/Restore

By carrying out the following steps, users can schedule the backup/restore 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/restore is attached.



Figure 5-27: Backup/Restore Screen

4. Expand the **Backup/Restore** section.
5. Select the check box of the LoadMaster or LoadMasters you wish to backup/restore and click the **Schedule** button.

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

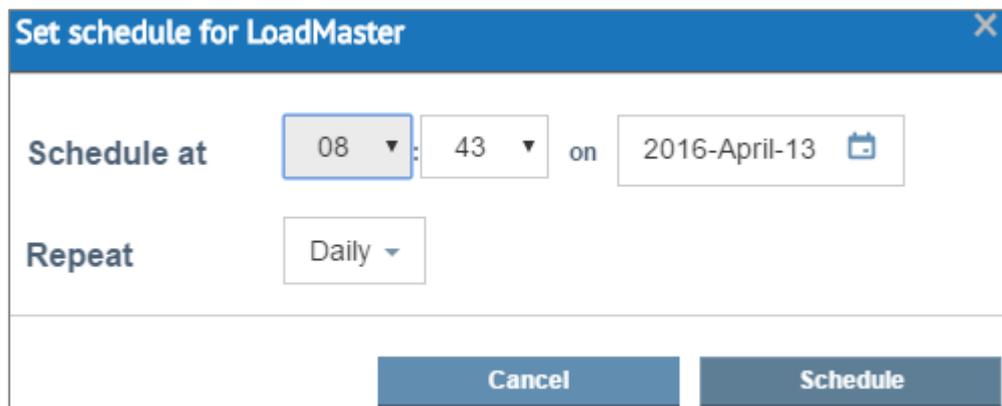


Figure 5-28: Schedule Screen

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

Tasks cannot be scheduled within one hour of each other.

7. Click **Schedule**.

5.5.5 Backup 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 all KEMP 360 Central administrative settings, all managed device settings, all repository files and all statistics data. To use the backup feature, follow the steps below:

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

▼ Backup

Central Settings The complete configuration database including credentials (calc...)

Password

Backup

▼ Restore

Backup File

kemp360_backup_20161213_115725...

Backup created 12 Dec 2016 on 172.22.0.9 with version 1.12.0.5 contains:

Central Settings

Password

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.

▼ Restore

Backup File

kemp360_backup_20161222_143527.zip

Select File

Remove File

Backup created 12 Dec 2016 on 10.154.153.94 with version 1.12.0.1521 contains:

Central Settings

Password

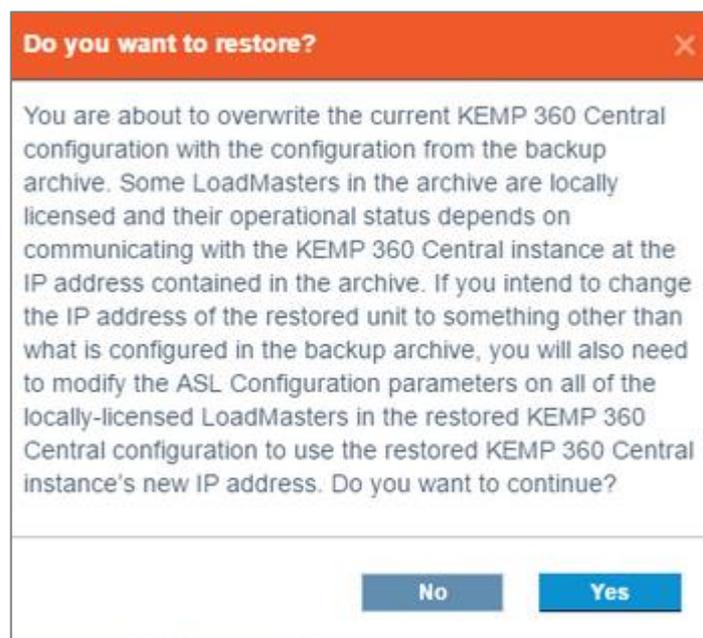
👁

Restore

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



4. Click **Yes** to the message that appears. For ASL 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.

5.5.6 Restoring KEMP 360 Central ASL Notes

If you are restoring an instance of KEMP 360 Central that uses ASL licensing, you may receive the message that appears in Step 4 of the previous procedure. Regardless of whether you choose to change the IP address of the newly restored unit or the unit on which the backup was taken, the managed devices (LoadMasters, and so on) that are defined on the newly restored unit, will continue to send syslogs, and so on, to the KEMP 360 Central IP address restored from the backup archive.

Therefore, when you select the system on which you will change the IP address, you can minimize the amount of additional changes you might need to make by selecting the system that you do not want to collect syslogs from. By doing this, you do not have to change IP addresses on all of the managed devices to point to the new IP address.

5.5.7 Configuring Syslog Collection from Managed Devices

You can configure KEMP 360 Central to collect 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.

5.5.8 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 **Section 14.1**.

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.

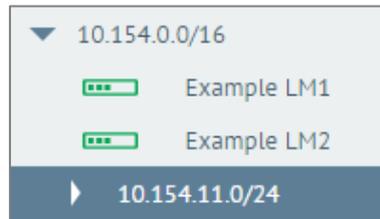


Figure 5-29: Select LoadMaster/network

3. Select the LoadMaster with the settings you wish to update.
4. Go to **Log Settings**.
5. Expand the **Syslog Options** section.

Log Settings

▼ Syslog Options

Emergency Host

Critical Host

Error Host

Warn Host

Notice Host

Info Host

Figure 5-30: Syslog Options

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.
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 host - multiple messages for the same error are sent to the same host.

5.5.8.1 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>

5.6 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 the KEMP 360 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.

Currently, HA is supported only on non-Service Provider License Agreement (SPLA) instances of KEMP 360 Central.

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 and receives log files from it also.

When configuring two KEMP360 Central instances into HA mode, both units must have at least one network defined for the initial synchronization to complete successfully. Remember, once the two units are initialized into HA mode, the configuration of the Preferred Master is propagated to the Preferred Slave, and the Preferred Slave's configuration is overwritten. 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 will always assume the master role in the HA configuration when it is available. The other unit will become the Preferred Slave; should the Preferred Master become unavailable, the Preferred Slave will take over from the master and return control to the Preferred Master once it is available again.

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

1. Go to the unit you want to make the slave.
2. Copy the HA Key of the peer you want to become the slave.
3. Open the master and copy the HA Key from the previous step into the **HA Key for the Other Peer** field.
4. Select the **Preferred Master** checkbox to ensure this device is the default master.
5. Type the IP address of the slave unit in the **IP Address for the Other Peer** field.

▼ HA Configuration

HA Key for this Peer **02839b96867e1c78d44eebeb0f841e978bae7ad7**

Disable

Preferred Master

IP Address for the Other Peer

HA Key for the Other Peer

Heartbeat Interval (seconds) **30**

Failed Heartbeat Threshold **2**

6. Click **Apply**.
7. Copy the HA Key of the Preferred Master.
8. Open the Preferred Slave and copy the HA Key from the previous step into the **HA Key for the Other Peer** field.
9. Type the IP address of the master unit in the **IP Address for the Other Peer** field.

▼ HA Configuration

HA Key for this Peer **e28a2d34a42293f2c6b30ef8b19736ae61d1b569**

Disable

Preferred Master

IP Address for the Other Peer

HA Key for the Other Peer

Heartbeat Interval (seconds) **30**

Failed Heartbeat Threshold **2**

10. Click **Apply**.

Both KEMP 360 HA units will 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 will 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 as long as you selected the **Preferred Master** checkbox when you configured it.

6 Service Configuration

In the **Service Configuration** section, users perform various management tasks.

6.1 Virtual Service Management

Users can view a list of Virtual Services, add or delete a Virtual Service. They can also modify the basic properties of individual Virtual Services as required.

6.1.1 Display the List of Virtual Services Attached to a LoadMaster

To view the list of Virtual Services attached to a LoadMaster, perform the following steps:

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



Figure 6-1: Service Configuration

2. Select the **Service Configuration** tab.
3. To display a particular Virtual Service from the list on the left, select the relevant network or LoadMaster.



Figure 6-2: List of Virtual Services attached to a LoadMaster

KEMP 360 Central displays a list of Virtual Services attached to the selected instance.

The status of each Virtual Service is indicated by the color of the circle beside the IP address. Green indicates the Virtual Service is up while a red status means the Virtual Service is down. Edit and delete icons are also available on this screen.

6.1.2 Add a Virtual Service

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



Figure 6-3: Service Configuration

2. Click **Service Configuration**.
3. Select the LoadMaster to which you wish to add the Virtual Service.

Add Virtual Service

Figure 6-4: Add a Virtual Service

4. Click **Add Virtual Service**.

Add new Virtual Service

Virtual Address/Port :

Protocol

Service Name

Figure 6-5: Virtual Services Basic Properties

5. Enter the **Virtual Address** of the Virtual Service you are adding.
6. Enter the **Port** of the Virtual Service. The valid range is 3 – 65530.

When adding a Virtual Service, you must use an IP Address and Port combination which is unique on the LoadMaster.

7. Enter a recognisable, unique name as the **Service Name**, if desired.
8. Select the appropriate **Protocol** from the drop-down list.



Figure 6-6: Apply Button

9. Click **Apply**. A message will appear to inform you that the Virtual Service has been successfully added.

6.1.3 Modify a Virtual Service

Occasionally you may need to make changes to the settings of a Virtual Service. Changes are made in the **Service Configuration** section of KEMP 360 Central.



Figure 6-7: System Configuration

1. Click **Service Configuration**.
2. Select the LoadMaster you wish to modify.



Figure 6-8: Pencil Icon

3. Click the pencil icon beside the Virtual Service you wish to modify.
4. Make any modifications, as needed.

Users can modify the following sections:

- Basic Properties
 - Real Servers
 - Standard Options
5. When the changes are made click **Apply**.



Figure 6-9: Deactivate Button

To deactivate a Virtual Service on this screen, click **Disable**.

6.1.4 Remove a Virtual Service

To delete a Virtual Service using KEMP 360 Central, in the **Service Configuration** section:

1. Click the **X** beside the Virtual Service you wish to delete. A dialog box appears asking you to confirm you wish to remove the Virtual Service.
2. Click **Remove**.

6.1.5 Migrate a Virtual Service

It is possible to migrate an existing Virtual Service from one LoadMaster to another LoadMaster. To do this, follow the steps below:

This migrates Real Servers, SubVSs and some other configuration settings. However, not all settings are currently migrated.



Figure 6-10: VS Motion Migrate

1. Click the **VS Motion Migrate** icon.

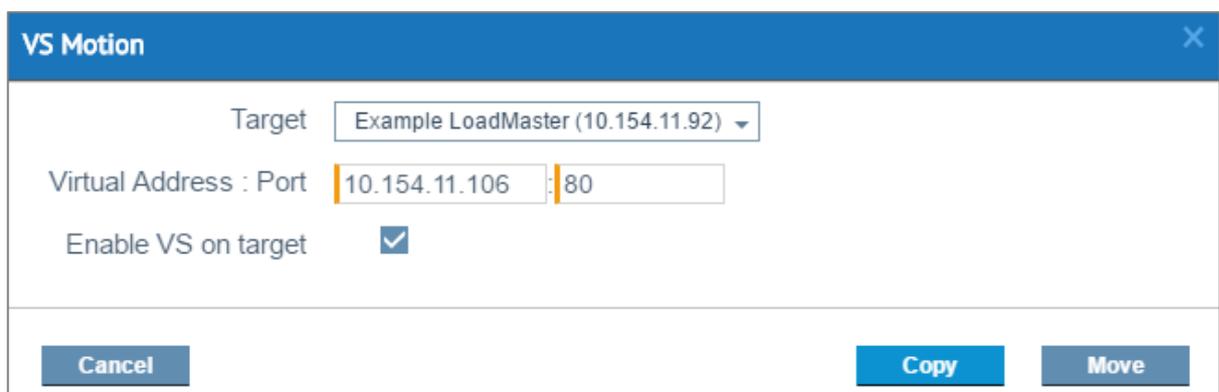


Figure 6-11: Copy

2. Select the **Target** LoadMaster.
3. Modify the **Virtual Address** and **Port**, if needed.

4. Decide whether or not to enable the Virtual Service on the target LoadMaster.
5. Click **Copy** to copy the Virtual Service, or **Move** to move it (that is, move it to the target LoadMaster and remove it from the original LoadMaster).

6.2 SubVS Management

KEMP 360 Central users can view a list of SubVSs and add or delete a SubVSs. Users can also modify the basic properties of an individual SubVS as required.

6.2.1 Display a List of SubVSs on a Virtual Service

KEMP 360 Central users can view the list of SubVSs. The following steps show how to access the list:

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



Figure 6-12: Service Configuration Tab

2. Select the **Service Configuration** tab.
3. Click the LoadMaster to which the Virtual Service whose SubVSs you wish to display are attached.



Figure 6-13: List of Available Virtual Services

KEMP 360 Central displays the list of Virtual Services attached to a LoadMaster.

4. Click the edit icon of the Virtual Service whose list of SubVSs you wish to view.



Figure 6-14: SubVSs Drop-down List

5. Expand the **SubVSs** section. The list of attached SubVSs is displayed.

6.2.2 Add a SubVS

KEMP 360 Central users can add a SubVS. The following steps show how to add a SubVS to a Virtual Service:

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



Figure 6-15: Service Configuration Tab

2. Select the **Service Configuration** tab.

3. Select the relevant LoadMaster.
4. Click the edit icon of the relevant Virtual Service.



Figure 6-15: Virtual Service Drop Down Lists

5. Expand the **Real Servers** section.



Figure 6-16: Buttons to add a new SubVS

6. Click the **Real Servers/SubVSs** toggle button.
7. Click the **New SubVS** button.

It is not possible to add a new SubVS if auto-scaling is enabled. To disable auto-scaling, click the **Real Servers/SubVSs** toggle button and remove the tick from the **Auto Scale** check box.

ID	Critical	Conn Limit	Weight			
22	<input type="checkbox"/>	0	1000			

Figure 6-17: A new SubVS has been added

An ID number has been assigned to the SubVS.

8. Click the edit icon of the SubVS you added.
9. Make modifications to the following sections, as needed:
 - Basic Properties
 - Real Servers
 - Standard Options
10. Click **Apply**.

6.2.3 Modify a SubVS

The following steps show how to modify a SubVS with KEMP 360 Central:

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



Figure 6-19: Service Configuration Tab

2. Select the **Service Configuration** tab.
3. Select the relevant LoadMaster.
4. Click the edit icon of the relevant Virtual Service.
5. Expand the **SubVSs** section.
6. Click the edit icon of the SubVS you wish to modify.
7. Make modifications to the **Basic Properties, Real Servers** and **Standard Options** sections as necessary.
8. Click **Apply**.

6.2.4 Delete a SubVS

The following steps show how to delete a SubVS with KEMP 360 Central:

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



Figure 6-20-: Service Configuration Tab

2. Select the **Service Configuration** tab.
3. Click the LoadMaster to which the Virtual Service and SubVS you wish to delete are attached.
4. Click the edit icon of the Virtual Service to which the SubVS you wish to delete is attached.
5. Expand the **SubVSs** section.
6. Click the **Delete** icon of the SubVS you wish to delete.

6.3 Real Server Management

KEMP 360 Central displays Real Servers which have been added to LoadMasters. As Real Servers are attached to Virtual Services, they are visible by accessing the **Edit** section of the individual Virtual Services listed in the **Service Configuration** tab.

KEMP 360 Central users can view a list of Real Servers. They may also add or delete a Real Server.

6.3.1 Display a List of Real Servers on a Virtual Service

KEMP 360 Central users can view the list of Real Servers. The following steps show how to access the list:

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



Figure 6-21 Service Configuration Tab

2. Select the **Service Configuration** tab.
3. Select the relevant LoadMaster.



Figure 6-22: List of Available Virtual Services

KEMP 360 Central displays the list of Virtual Services attached to a LoadMaster.

4. Click the edit icon of the relevant Virtual Service.



Figure 6-23: Real server

5. Expand the **Real Servers** drop-down list.



Figure 6-24: The Real Server Attached to the Selected Virtual Service

6.3.2 Add a Real Server

Follow the instructions below to add a Real Server to a Virtual Service:

1. For the LoadMaster you wish to modify, display the list of Virtual Services attached (see **Section 6.1.1**).
2. Click the edit icon of the Virtual Service to which you wish to add the Real Server.
3. Expand the **Real Server** section.
4. Ensure the **Real Servers/SubVSs** toggle is set to Real Servers.



Figure 6-25: Add a New Real Server

5. Click the **New Real Server** button.
6. Enter the following values in the appropriate text box:
 - IP
 - Port
 - Conn Limit
 - Weight
7. Click **Save**.

6.3.3 Modify a Real Server

This section shows how to modify an existing Real Server:

1. For the LoadMaster you wish to modify, display the list of Virtual Services attached (see **Section 6.1.1**).
2. Click the edit icon of the Virtual Service to which the Real Server you wish to modify is attached.
3. Expand the **Real Servers** section.
4. Click the edit icon of the Real Server which you wish to modify.
5. Modify any or all of the following values which display:
 - Port
 - Conn Limit
 - Weight
6. Click **Save**.

6.3.4 Remove a Real Server

This section shows how to remove a Real Server from a Virtual Service:

1. For the LoadMaster you wish to modify, display the list of Virtual Services attached (see **Section 6.1.1**).
2. Click the edit icon of the relevant Virtual Service.
3. Expand the **Real Servers** section.
4. Click the **X** symbol beside the Real Server you wish to remove.

6.3.5 Health Check

The screenshot shows a 'Health Check' configuration panel. It contains the following elements:

- Protocol : Port**: A dropdown menu set to 'HTTP Protocol' and an empty port input field.
- URL**: An empty text input field.
- Status code**: An empty text input field.
- Use HTTP/1.1**: An unchecked checkbox.
- HTTP Method**: A dropdown menu set to 'HEAD'.
- Custom Headers**: A section with a 'Hide Custom Headers' button and an 'Add custom header' button.
- Enhanced Options**: An unchecked checkbox.
- Apply**: A blue button at the bottom right.

Figure 6-26: Health Check

You can configure the health check parameters for the Real Servers in the **Health Check** section. For further information on health checking in general, and detailed descriptions on each of these fields, please refer to the **Health Checking, Feature Description**.

7 Monitoring

The **Monitoring** section of KEMP 360 Central provides status and performance statistics for connected appliances. Users can oversee the health of and activity across their networks, subnetworks and devices. All statistics update every 5 minutes.



Figure 7-1: Monitoring

7.1 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, the number of Virtual Services that are down and the number of Real Servers that are down.

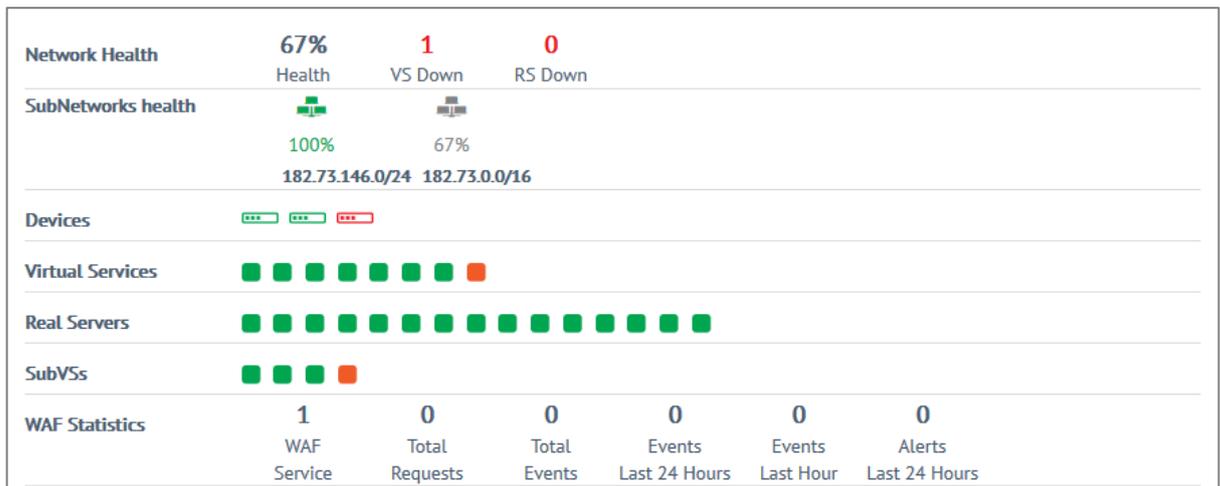


Figure 7-2: Overall Network Health

To view the monitoring section of an individual KEMP 360 Central device, first click on the relevant network or device and then click **Monitoring** in the top-right of the screen.

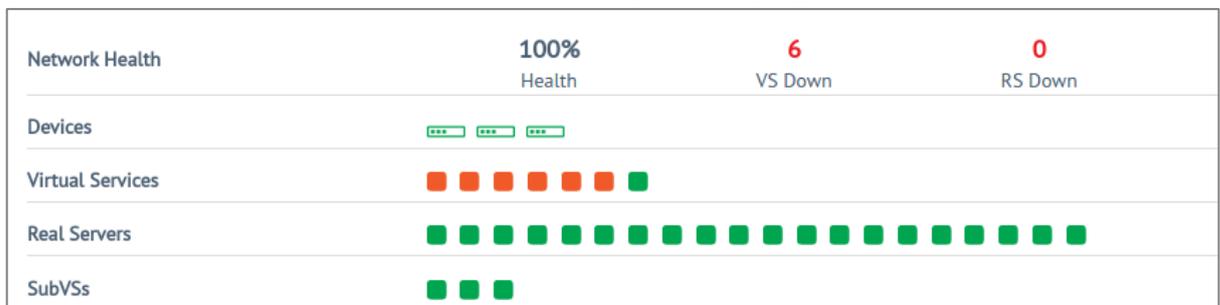


Figure 7-3: Network Health



Figure 7-3: Network Metrics Screen

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 being monitored. The network health percentage is calculated using the number of devices with an UP status on the network, against the total number of devices in that network.

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.

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 Activation Server functionality).

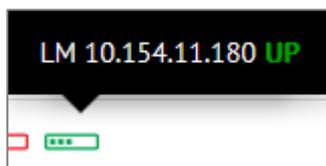


Figure 7-4: LoadMaster Status

Hovering over the device icons displays the IP address and status of that device.

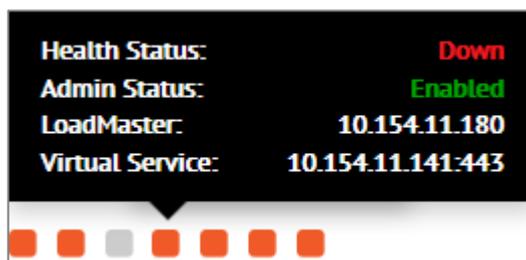


Figure 7-5: Virtual Services Status

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

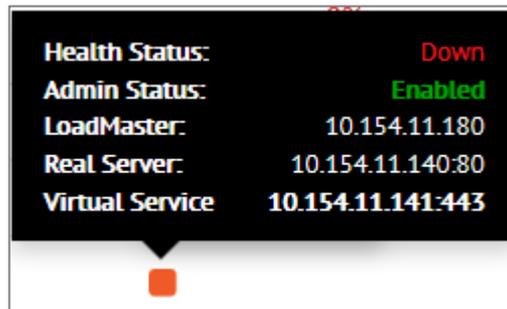


Figure 7-6: Real Server Status

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 of individual Real Servers. Hover help, also displays the IP address of the individual Virtual Service and device, to which it is attached.

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:

Virtual Services			
● 10.35.0.6:80	UDP	● 10.35.26.50:80	TCP
Real Servers			
● 10.154.120.59:80	● 10.154.120.60:80	● 10.154.120.59:81	● 10.154.120.60:81
● 10.154.120.59:82	● 10.154.120.60:82	● 10.154.120.59:83	● 10.154.120.60:83
● 10.154.120.59:80	● 10.154.120.60:80	● 10.154.120.59:81	● 10.154.120.60:81
● 10.154.120.59:82	● 10.154.120.60:82	● 10.154.120.59:83	● 10.154.120.60:83
● 10.154.120.59:80	● 10.154.120.60:80	● 10.154.120.59:81	● 10.154.120.60:81

Figure 7-7: Status of Virtual Services and Real Servers on an Individual LoadMaster

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.

For more information on WAF Statistics, refer to **Non-Local Licenses & Subscriptions**.

In the Non-Local Licenses & Subscriptions panel you can quickly identify LoadMasters that are approaching or have passed an expiration date. The Non-Local Licenses & Subscriptions panel displays the number of Subscriptions and Non-Subscription licenses and these are color coded as follows:

Red: Expired

Orange: 7 Days

Yellow: 30 Days

Blue: 60 Days

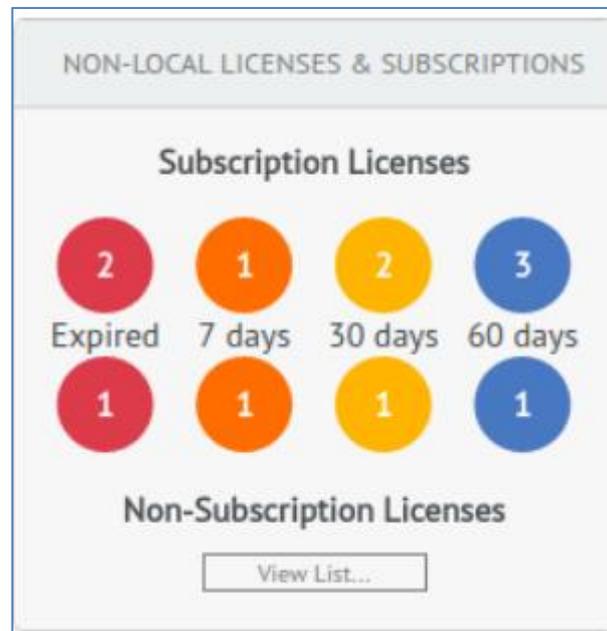


Figure 3-5: Non-Local Licenses & Subscriptions Widget

This feature does not include licenses activated by the KEMP 360 Central Activation Server Local (ASL) feature; these are reported in a separate dashboard widget.

- You will receive an alert on the Non-Local Licenses & Subscriptions widget when a subscription expiration has occurred (or is about to occur within 7, 30 or 60 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 Non-Local Licenses & Subscriptions widget, you can view the Licenses table, which provides information on the type of license and the expiration date.
- Licenses and subscriptions that are expired are shown in red in the table. In the **Non-Local Licenses & Subscriptions** panel you can quickly identify LoadMasters that are approaching or have passed an expiration date. The Non-Local Licenses & Subscriptions panel displays the number of Subscription and Non-Subscription licenses and these are color coded as follows:

Red: Expired

Orange: 7 Days

Yellow: 30 Days

Blue: 60 Days



Figure 3-5: Non-Local Licenses & Subscriptions Widget

This feature does not include licenses activated by the KEMP 360 Central Activation Server Local (ASL) feature; these are reported in a separate dashboard widget.

- You will receive an alert on the Non-Local Licenses & Subscriptions widget when a subscription expiration has occurred (or is about to occur within 7, 30 or 60 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 Non-Local Licenses & Subscriptions widget, you can view the Licenses table, which provides information on the type of license and the expiration date.
- Licenses and subscriptions that are expired are shown in red in the table.

System Administration

- ▶ System Reboot
- ▶ Templates
- ▶ Update LoadMaster Firmware
- ▶ Backup/Restore
- ▼ Licenses

IP Address	Nickname	License or Subscription	Expiration Date
10.35.26.22		Classic	2018-02-14 05:00

Application Health.



Figure 7-8: Network Metrics

The **Monitoring** section displays three graphs.

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 year. 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.

Users should note that whichever device or network is highlighted in the left side-bar is the device or network which they are working with. Please ensure you choose the correct one.

7.2 System Statistics



Figure 7-9: System Statistics - List View

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%).

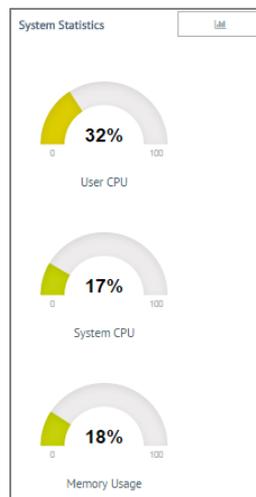


Figure 7-10: System Statistics Gauges

To display the gauges as shown in **Figure 7-10: System Statistics Gauges**, users should click the button with the gauge icon as shown in **Figure 7-9: System Statistics - List View**.

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.

7.3 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. **Section 5** of this document has details about those features. The section below relates to the **Logging** screen that is also available in the **Global Repository**.



Figure 7-11: Global Repository

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

7.4 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.

Time Generated (UTC)	Source IP	Facility	Severity	Process ID	App Name	Message
2016-09-28 14:47:25	10.154.11.100	5	6	-	1.4.1	restart.
2016-09-28 14:47:25	10.154.11.100	4	3	684	sshd	error: Bind to port 22 on 10.154.11.110 failed: Cannot assign requested address.

Figure 7-12: Logging Screen

There are three main sections:

- Source
- Filter
- Log Search Results

7.4.1 Source

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

The screenshot shows a 'Source' configuration panel. It contains the following fields:

- Logfile:** A dropdown menu with 'Remote Logs' selected.
- Range:** A dropdown menu with 'Time Range' selected.
- From:** A date field showing '2016-January-05' and a time field showing '00'.
- To:** A date field showing '2016-February-09' and a time field showing '00'.

Figure 7-13: Source Section

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.

7.4.2 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	

Table 6-1: Levels of Severity

- 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.

Figure 7-14: Filter by device

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**.

7.4.3 Log Search Results

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

Log Search Results							Export	Search
Time Generated (UTC)	Source IP	Facility	Severity	Process ID	App Name	Message		
2016-10-04 10:39:49	10.0.255.4	0	4	-	kernel	Cannot find map file.		
2016-10-04 10:39:49	10.0.255.4	0	4	-	kernel	Cannot build symbol table - disabling symbol lookups		
2016-10-04 12:15:23	10.0.255.5	0	4	-	kernel	Cannot find map file.		
2016-10-04 12:15:23	10.0.255.5	0	4	-	kernel	Cannot build symbol table - disabling symbol lookups		
2016-10-04 12:24:28	10.0.255.5	0	4	-	kernel	hrtimer: interrupt took 25340400 ns		
NO MORE DATA								

Figure 7-4: Log Search Results

- **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.

```

syslog.txt - Notepad
File Edit Format View Help
[[Time Generated] [Source] [Source IP] [Facility] [Severity] [Process ID] [App Name] | Message
[2016-09-28T14:50:59.203852+00:00] [10.154.11.100] [10.154.11.100] [5] [6] [-] [1.4.1] | restart.
[2016-09-28T14:50:59.244335+00:00] [10.154.11.100] [10.154.11.100] [4] [5] [-] [access] | API K360Central_10.154.190.130_1 (10.154.1
[2016-09-28T14:50:59.251043+00:00] [10.154.11.100] [10.154.11.100] [4] [5] [-] [access] | API bal (10.154.190.130) set 'param=syslog
[2016-09-28T14:50:59.587111+00:00] [10.154.11.100] [10.154.11.100] [0] [6] [-] [kernel] | Kernel log daemon terminating.
[2016-09-28T14:50:59.651112+00:00] [10.154.11.100] [10.154.11.100] [5] [6] [-] [on] | signal 15
[2016-09-28T14:50:59.751046+00:00] [10.154.11.100] [10.154.11.100] [5] [6] [-] [1.4.1] | restart.
[2016-09-28T14:50:59.788729+00:00] [10.154.11.100] [10.154.11.100] [4] [5] [-] [access] | API K360Central_10.154.190.130_1 (10.154.1
[2016-09-28T14:51:00.102421+00:00] [10.154.11.100] [10.154.11.100] [0] [6] [-] [kernel] | Kernel log daemon terminating.
[2016-09-28T14:51:00.166636+00:00] [10.154.11.100] [10.154.11.100] [5] [6] [-] [on] | signal 15
[2016-09-28T14:51:00.270517+00:00] [10.154.11.100] [10.154.11.100] [5] [6] [-] [1.4.1] | restart.
[2016-09-28T14:51:00.309571+00:00] [10.154.11.100] [10.154.11.100] [4] [5] [-] [access] | API K360Central_10.154.190.130_1 (10.154.1
[2016-09-28T14:51:00.664532+00:00] [10.154.11.100] [10.154.11.100] [0] [6] [-] [kernel] | Kernel log daemon terminating.
[2016-09-28T14:51:00.728368+00:00] [10.154.11.100] [10.154.11.100] [5] [6] [-] [on] | signal 15
[2016-09-28T14:51:00.828610+00:00] [10.154.11.100] [10.154.11.100] [5] [6] [-] [1.4.1] | restart.
[2016-09-28T14:51:00.867868+00:00] [10.154.11.100] [10.154.11.100] [4] [5] [-] [access] | API K360Central_10.154.190.130_1 (10.154.1
[2016-09-28T14:51:01.184277+00:00] [10.154.11.100] [10.154.11.100] [0] [6] [-] [kernel] | Kernel log daemon terminating.
[2016-09-28T14:51:01.248248+00:00] [10.154.11.100] [10.154.11.100] [5] [6] [-] [on] | signal 15
[2016-09-28T14:51:01.350377+00:00] [10.154.11.100] [10.154.11.100] [5] [6] [-] [1.4.1] | restart.
[2016-09-28T14:51:01.387491+00:00] [10.154.11.100] [10.154.11.100] [4] [5] [-] [access] | API K360Central_10.154.190.130_1 (10.154.1
[2016-09-28T14:51:01.697074+00:00] [10.154.11.100] [10.154.11.100] [0] [6] [-] [kernel] | Kernel log daemon terminating.
[2016-09-28T14:51:01.761796+00:00] [10.154.11.100] [10.154.11.100] [5] [6] [-] [on] | signal 15
[2016-09-28T14:51:01.860803+00:00] [10.154.11.100] [10.154.11.100] [5] [6] [-] [1.4.1] | restart.
[2016-09-28T14:51:01.891563+00:00] [10.154.11.100] [10.154.11.100] [4] [5] [-] [access] | API K360Central_10.154.190.130_1 (10.154.1
[2016-09-28T14:51:02.194273+00:00] [10.154.11.100] [10.154.11.100] [0] [6] [-] [kernel] | Kernel log daemon terminating.
[2016-09-28T14:51:02.257322+00:00] [10.154.11.100] [10.154.11.100] [5] [6] [-] [on] | signal 15
[2016-09-28T14:51:02.357951+00:00] [10.154.11.100] [10.154.11.100] [5] [6] [-] [1.4.1] | restart.
[2016-09-28T14:51:02.392461+00:00] [10.154.11.100] [10.154.11.100] [4] [5] [-] [access] | API K360Central_10.154.190.130_1 (10.154.1
[2016-09-28T14:51:07.371218+00:00] [10.154.11.100] [10.154.11.100] [0] [6] [-] [kernel] | klogd 1.4.1, log source = /proc/kmsg starte
[2016-09-28T14:51:07.371262+00:00] [10.154.11.100] [10.154.11.100] [0] [4] [-] [kernel] | Cannot find map file.
[2016-09-28T14:51:07.371262+00:00] [10.154.11.100] [10.154.11.100] [0] [6] [-] [kernel] | No module symbols loaded - kernel modules n
[2016-09-28T14:51:07.371262+00:00] [10.154.11.100] [10.154.11.100] [0] [4] [-] [kernel] | Cannot build symbol table - disabling symbo
[2016-09-28T14:51:07.942368+00:00] [10.154.11.100] [10.154.11.100] [1] [4] [1073] [vmsvc] | [ warning] [guestinfo] Failed to get nic
[2016-09-28T14:51:07.942523+00:00] [10.154.11.100] [10.154.11.100] [1] [4] [1073] [vmsvc] | [ warning] [guestinfo] Failed to get vmst
[2016-09-28T14:51:37.942965+00:00] [10.154.11.100] [10.154.11.100] [1] [4] [1073] [vmsvc] | [ warning] [guestinfo] Failed to get nic
[2016-09-28T14:51:37.943188+00:00] [10.154.11.100] [10.154.11.100] [1] [4] [1073] [vmsvc] | [ warning] [guestinfo] Failed to get vmst
    
```

Figure 7-5: Log Search Results

8 Access Control

You can administer users in the **User Management** screen, which you can 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 **read write** and these can be set for both **Service Configuration** and **System Configuration**.



Figure 8-1: Access Control

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.

8.1 User Management



User Name	Email	Status	Operation
admin			 
Example User	exampleuser@example.com	<input checked="" type="checkbox"/>	 

Figure 8-2: User Management

The **User Management** screen lists all KEMP 360 Central users. Here, you can modify, delete and disable users. You can add a new user by clicking the **Add new User** button and filling out the details. As an admin user, you can add new users and select their status as read only or read-write.

▼ User details

Username	<input type="text" value="Example User"/>
Email	<input type="text" value="exampleuser@example.com"/>
Password	<input type="password" value="****"/>
Confirm Password	<input type="password" value="****"/>
Active	<input checked="" type="checkbox"/>

▼ User Permissions

Permission Name	Read only	Write
Service Configuration	<input checked="" type="radio"/>	<input type="radio"/>
System Configuration	<input checked="" type="radio"/>	<input type="radio"/>

Figure 8-3: Modify User

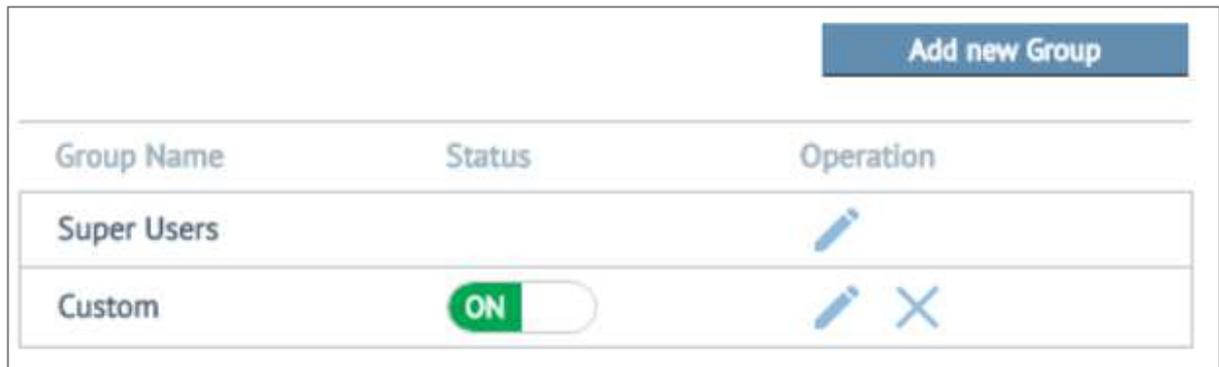
In the **Modify User** screen, you can update various details about the user including their password, email address and permissions. By default, user permissions are set to read only (for details on setting your password, see the **Appendix: Password Information**).

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.

8.2 Group Management

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



Group Name	Status	Operation
Super Users		
Custom	<input checked="" type="checkbox"/>	 

Figure 8-4: Group Management

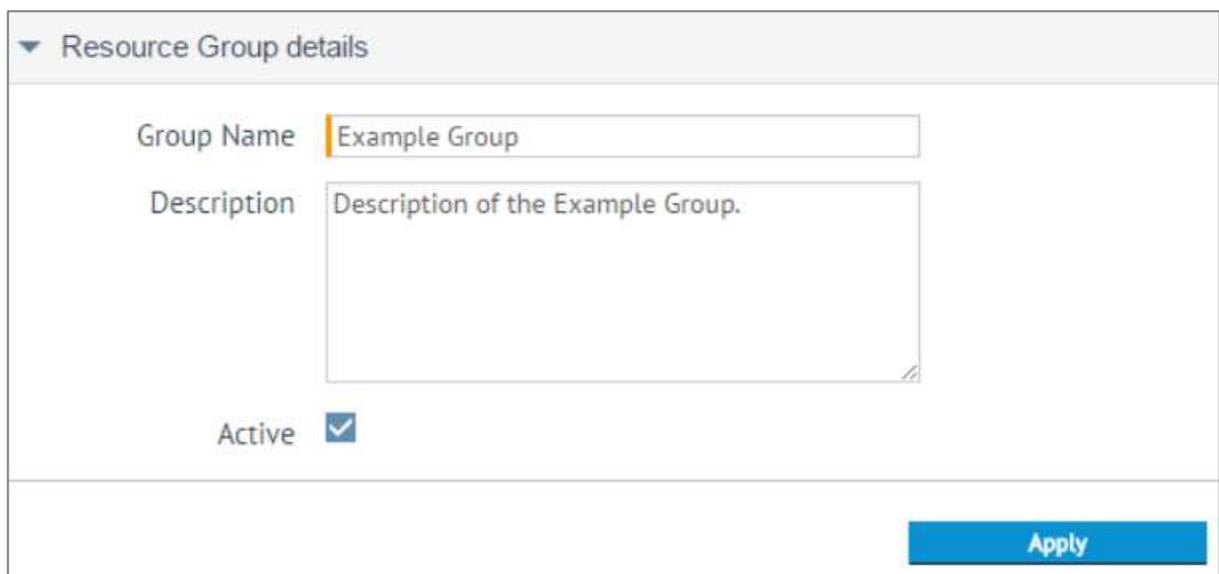
The **Group Management** screen lists any existing user groups. The **Super Users** group cannot be disabled or deleted because this is a default system group.

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.

8.2.1 Group Details



▼ Resource Group details

Group Name

Description

Active

Figure 8-5: Add Group

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.

8.2.2 Group Members

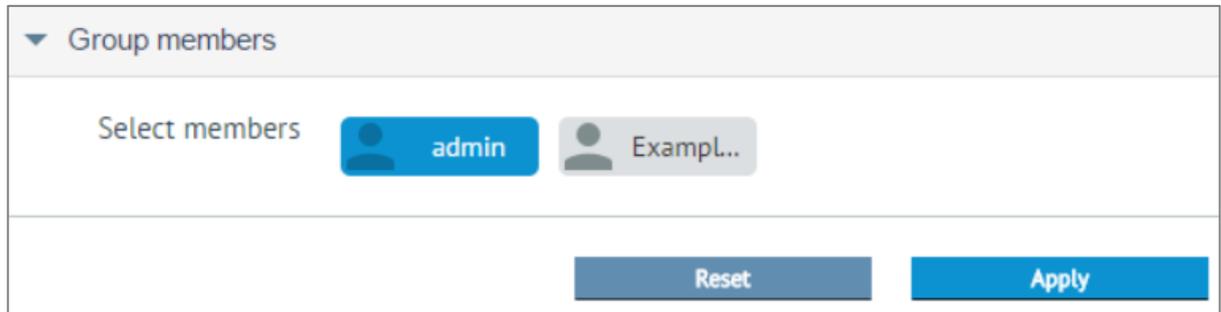


Figure 8-6: Group members

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.

Table 8-1: User group statuses

8.2.3 Group Resources

▼ Group resources

Select resources ▼ 10.154.11.100

- 10.154.11.143
- 10.154.11.141
- 10.154.11.141
- 10.154.11.141
- 10.154.11.141
- 10.154.11.142

Apply

Figure 8-7: 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.

9 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.



Figure 10-1: Cog icon

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

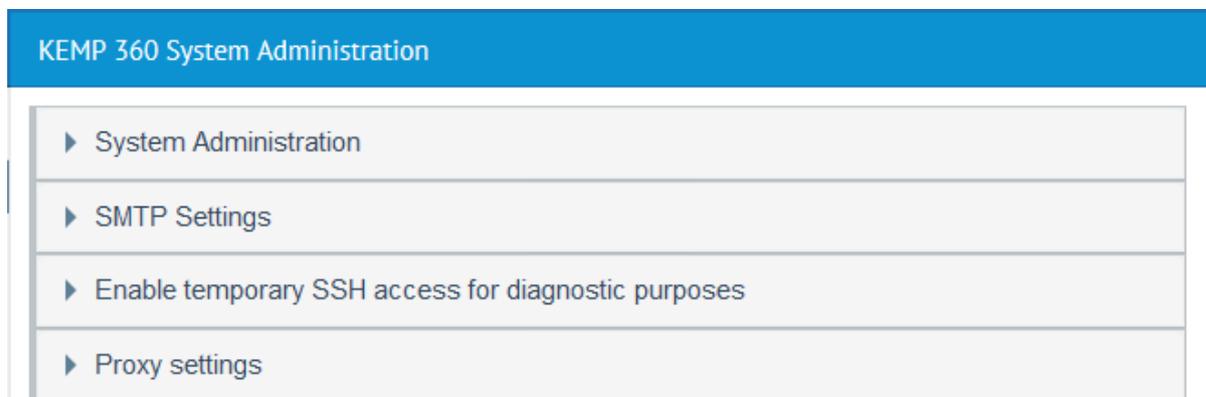


Figure 10-2: KEMP 360 Central System Administration

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

9.1 Reboot/Shutdown KEMP 360 Central

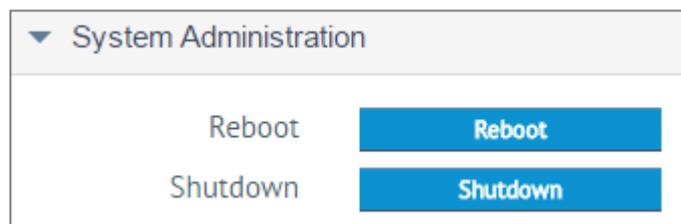


Figure 10-3: KEMP 360 Central Administration

This section of the 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.

9.2 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 critical errors occur, such as a LoadMaster going down.

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

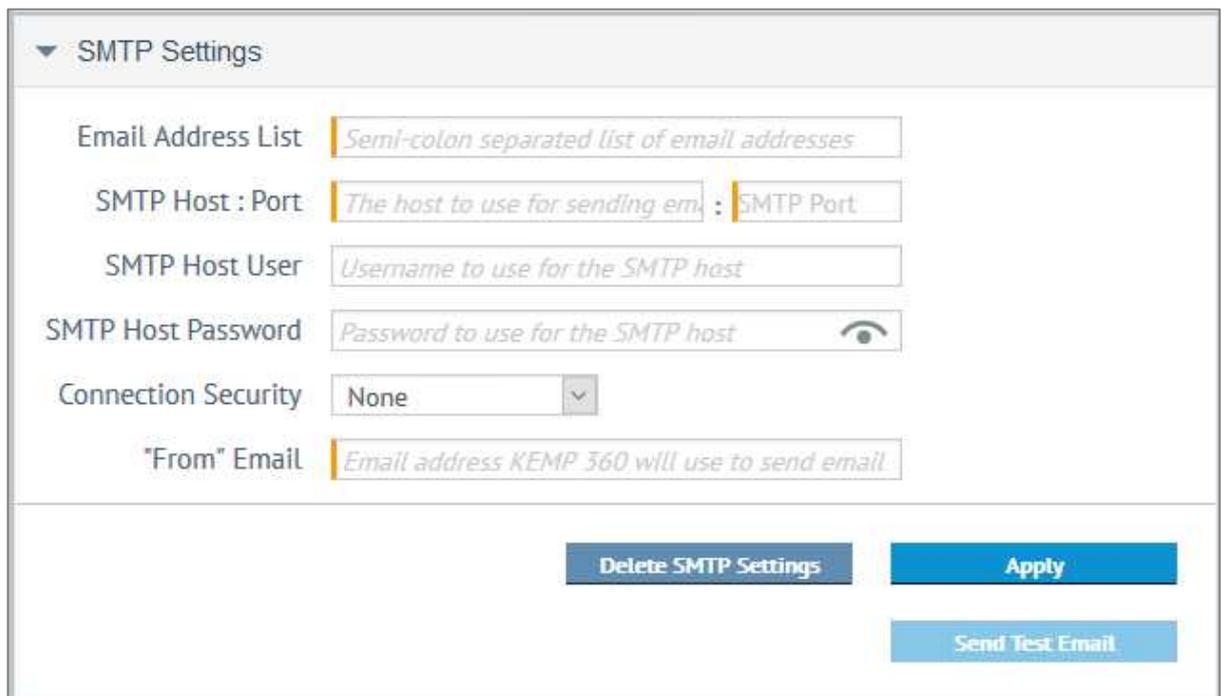


Figure 10-: SMTP Settings

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.

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. Click the **Apply** button.

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.

9.3 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 administrator with a once-off activation code provided by KEMP Support. SSH access is enabled for 24 hours or until disabled by the administrator.

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.

▼ Enable temporary SSH access for diagnostic purposes

To assist with issue diagnosis and resolution, the KEMP support team may need to enable temporary 'shell' access using SSH. The KEMP support team will guide you through this process and provide the once-off code to temporarily enable SSH access.

SSH Public Key Save SSH Key

Access Code Regenerate

Pass Code

Revoke Access Grant Access

Figure 9-5: Enter SSH key

4. Enter an **SSH Public Key** code in the **SSH Public Key** text box and click **Save SSH Key**.
5. To generate the access passcode, click **Regenerate**.
6. Contact KEMP Support and provide them with the generated passcode.
7. KEMP Support will provide you with a code which grants diagnostic SSH access.
8. Enter the code received from KEMP Support into the **Pass Code** text box and then click **Grant Access**.
9. If you wish to revoke access to the KEMP 360 Central instance, click **Revoke Access**.

9.4 Proxy Settings

▼ Proxy settings

HTTP(S) Proxy : Port :

Test Clear Apply

Figure 9-6: Proxy settings

Configuring the settings in this section will allow KEMP 360 Central to access other networks using a HTTP(S) Proxy. Specify either an IP address or a domain here. Click the **Test** button to check if the proxy server is reachable.

10 License Management

The KEMP 360 Central license can be updated, if required. This would be required if, for example, if you upgrade to premium support.

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



Figure 10-1: Cog icon

1. In the bottom-left corner, click the cog icon (you can also click the ? icon).
2. Click **License Management**.
3. You can use online or offline licensing to update the KEMP 360 Central license. For further information and step-by-step instructions on each method, refer to the **KEMP 360 Central Licensing, Feature Description**.

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.

11 Firmware Management

You can update the KEMP 360 Central firmware using the **Firmware Management** screen. There are two methods to update the firmware – online or offline. Refer to the sub-sections below for further information.

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.

11.1 Update the KEMP 360 Central Firmware - Online Method

To update the KEMP 360 Central firmware using the online method, follow the steps below:



Figure 11-1: Cog icon

1. In the KEMP 360 Central UI, click the cog icon in the bottom-left corner.
2. Click **Firmware Management**.

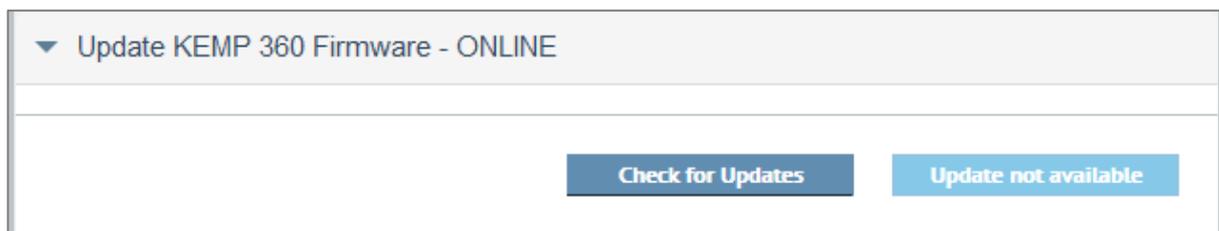


Figure 11-2: Check for Updates

3. Click **Check for Updates**.

If there are no updates available, a message is displayed to inform you.

4. Click **Download & Install** to proceed with the update.

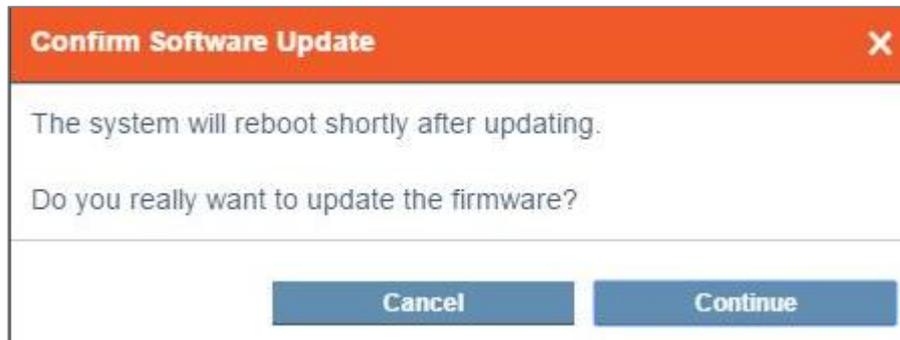


Figure 11-3: Confirm update

5. A message appears asking if you want to proceed with the update. Click **Continue** to proceed.
You can view the progress of the upload in the progress bar.



Figure 11-4: Rebooting

6. After the update, KEMP 360 Central reboots.

11.2 Update the KEMP 360 Central Firmware – Offline Method

A firmware update patch file is required to update the firmware using the offline method. Contact KEMP Support to get the patch file.

To update the KEMP 360 Central firmware using the offline method, follow the steps below:



Figure 11-5: Cog icon

1. In the KEMP 360 Central UI, click the cog icon in the bottom-left corner.
2. Click **Firmware Management**.

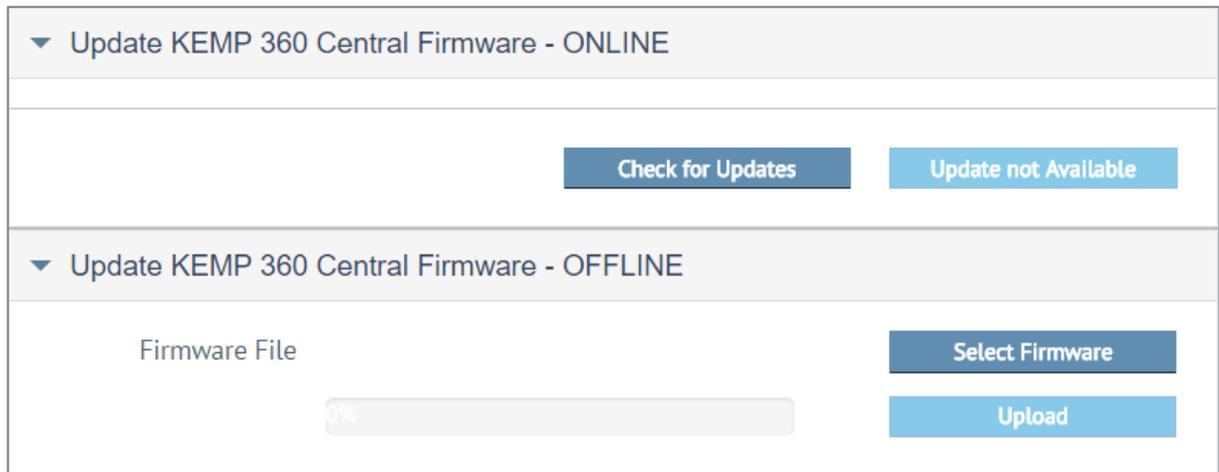


Figure 11-6: Select Firmware

3. Click **Select Firmware**.
4. Browse to and select the firmware update file.
5. Click **Upload & Install**.

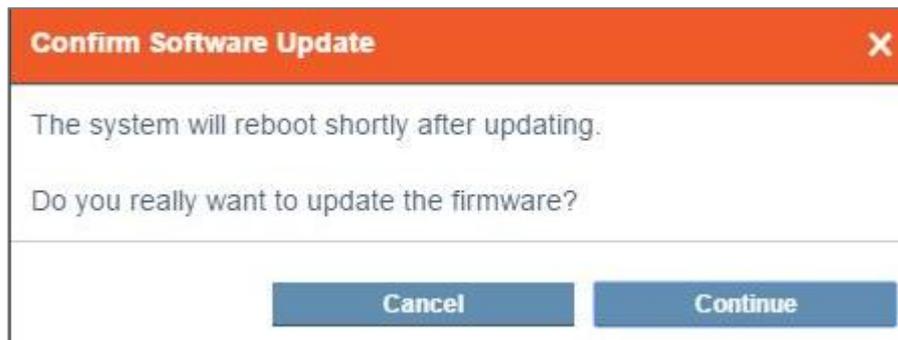


Figure 11-7: Confirm update

6. A message appears asking if you want to proceed with the update. Click **Continue** to proceed.
You can view the progress of the upload in the progress bar.



Figure 11-8: Rebooting

7. After the update, KEMP 360 Central reboots.

12 Metered Licensing Management

This section displays ASL information and metrics data on LoadMasters under the control of KEMP 360 Central. For further information, refer to the **Metered Licensing Management, Feature Description**.

12.1 Instances

▼ Instances					
Max ASL Activations Available: 100					
Current Number of ASL Activations: 0					
MAC Address	LoadMaster Version	Status	Activation Date	Boot Date	Last Kill Date
00155dbe6742	7.1.34.1.12...	DISABLED	2016-06-23 12:58:52	2016-06-23 04:32:52	2016-06-23 13:04:14
00155dbe6748	7.1-32b-95	ACTIVE	2016-06-24 10:50:25	2016-06-24 04:30:52	Invalid date

Figure 12-1: ASL Instances

KEMP 360 Central records and stores the following for each Activation Server Local (ASL) instance:

- **MAC Address** – Each device has a unique media access control (MAC) address to identify it for communications purposes.
- **LoadMaster Version** – Firmware version installed on the LoadMaster.
- **Status** – There are two possible statuses: **Active** and **Disabled**.
- **Activation Date** – The date the particular ASL instance was first activated.
- **Boot Date** – The date the particular ASL instance was last booted.
- **Last Kill Date** – The date the particular ASL instance was last killed.

12.2 Report Data

In this section, users can view a report displaying the number of active ASL instances. This report can be filtered by using a date range. To view a graphical representation of the report, click **View MELA Report** (MELA = Metered Enterprise Licensing Agreement).

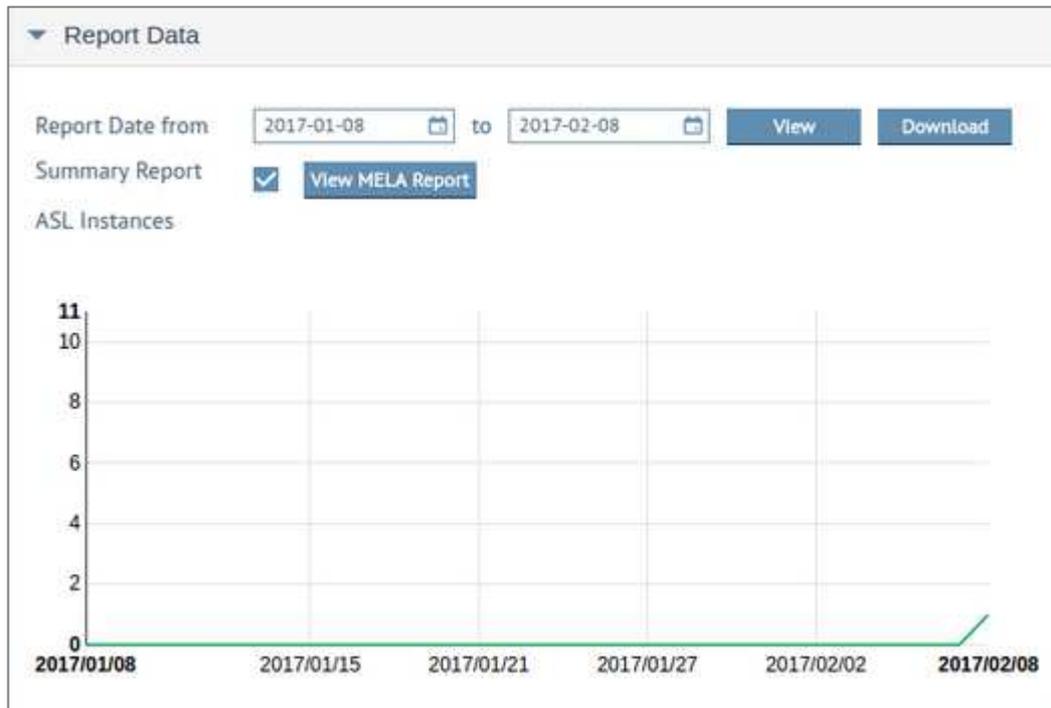


Figure 12-2: Report Data

Reports can also be downloaded in zip format by clicking **Download**. The downloaded zip file contains three CSV files:

- An event report that displays events and the number of active ASL instances at the time of the event. The events recorded are as follows:
 - Activation: An ASL LoadMaster has been activated using this KEMP 360 Central instance
 - Deactivation: An ASL LoadMaster on this KEMP 360 Central instance has been deactivated
 - Sync (Discrepancy): KEMP 360 Central has detected a discrepancy between the previously recorded instance count and the actual instance count, and has corrected the error
 - Sync (No Discrepancy): No discrepancy has been detected. In the absence of other ASL events, this serves as the instance count for any given day. The sync task is performed in the following circumstances:
 - If KEMP 360 Central is upgraded to v1.6 or later
 - Daily at 12 pm
- An SSL Transactions Per Second (TPS) report
- A report displaying the number of Virtual Service bytes transferred

These reports include minute-by-minute data from 00.00 hours of the start date selected up to the minute the report is run. To get a full report, leave the **Summary** check box cleared. To get a summarized report, select the **Summary** check box. This report produces an archive containing three files:

- Daily peak TPS per ASL LoadMaster per day
- Daily peak throughput (bytes per second) per ASL LoadMaster per day
- All ASL activations or deactivations (and the number of active ASL instances at the time)

To view a MELA Report for a specific date range, select the date range then click **View MELA Report**.

This report provides you with a graphical representation of the information such as the maximum number of ASL instances that were recorded during the report period, the maximum number of SSL transactions and the maximum throughput for each individual day. The report displays usage data, which enables you to examine and validate the periodic billing statements you receive from KEMP for metered licensing.

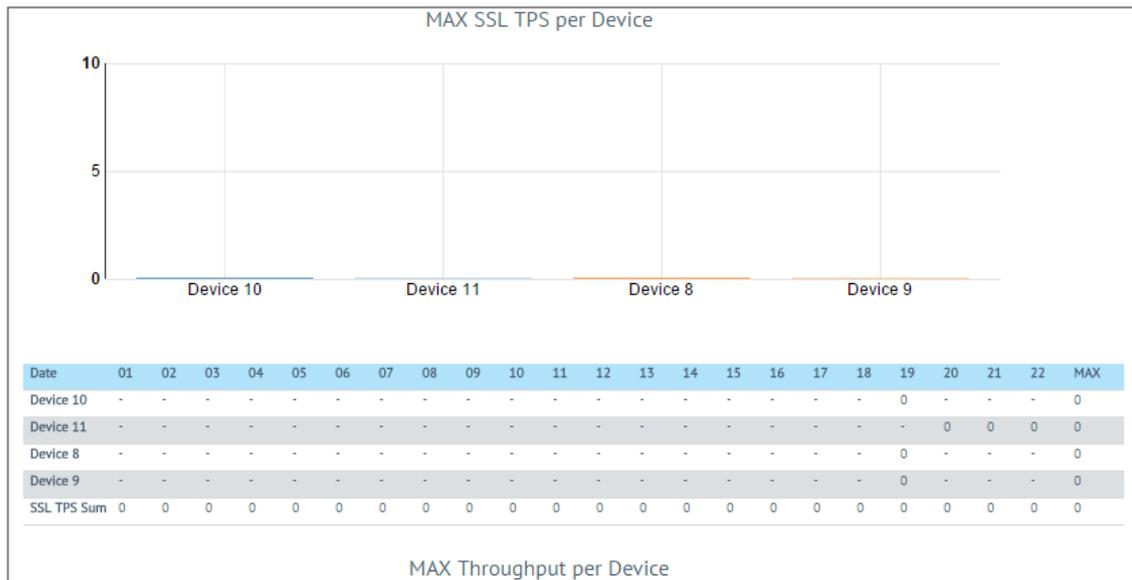


Figure 12-3: Max SSL TPS per Device

There is also a table under the graph that displays the information in tabular format. You can also view detailed individual graphs on the maximum number of SSL transactions per device. In

In addition, you can view the MAX throughput per device and see the aggregate used over the time period.

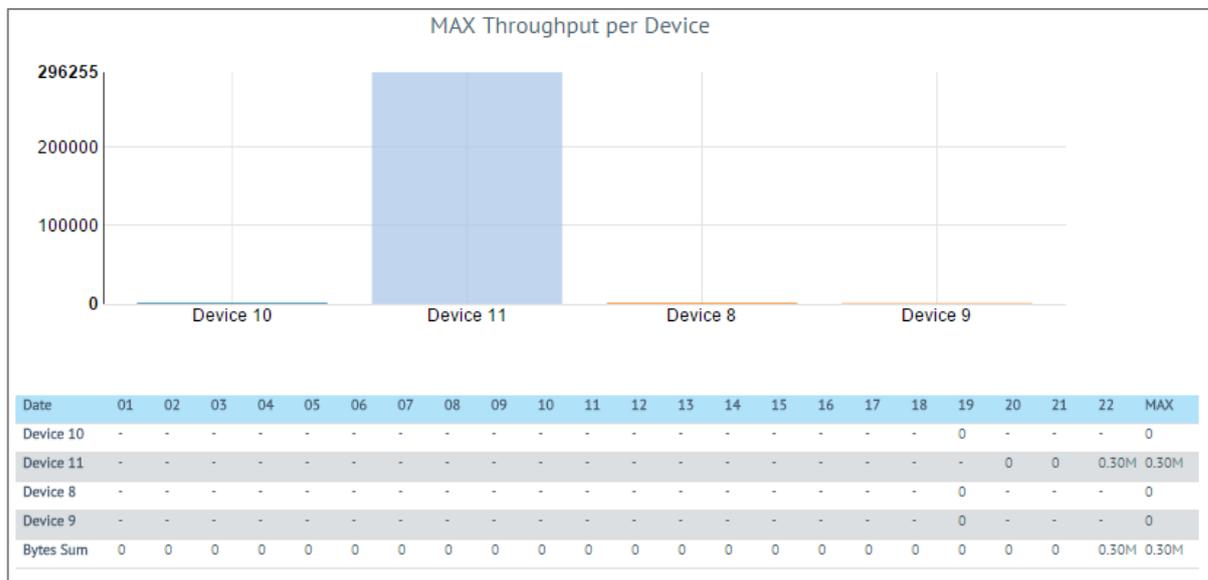


Figure 12-4: MAX throughput per device

13 Scheduled Actions

In this section, users can view which, when and how often, actions are scheduled to take place. They can also edit or delete scheduled actions. The section displays all actions scheduled to take place on any and all LoadMasters that are controlled by the particular KEMP 360 Central instance.

13.1 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**.

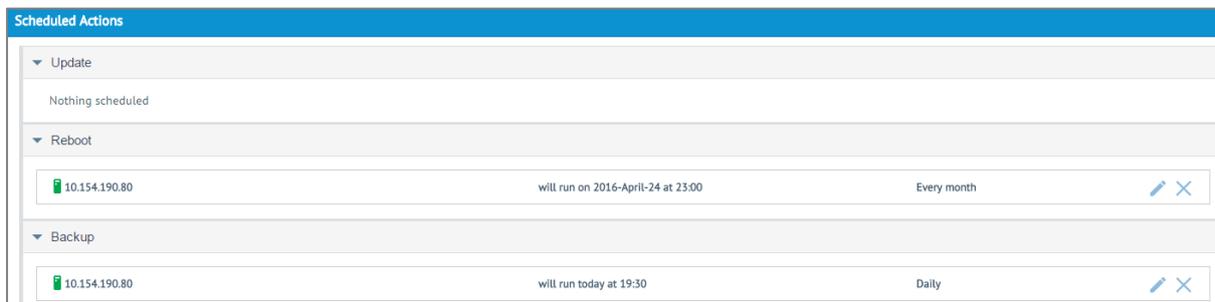


Figure 13-1: Scheduled Actions Screen

A full list of scheduled firmware updates, reboots and backups displays.

13.2 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**.

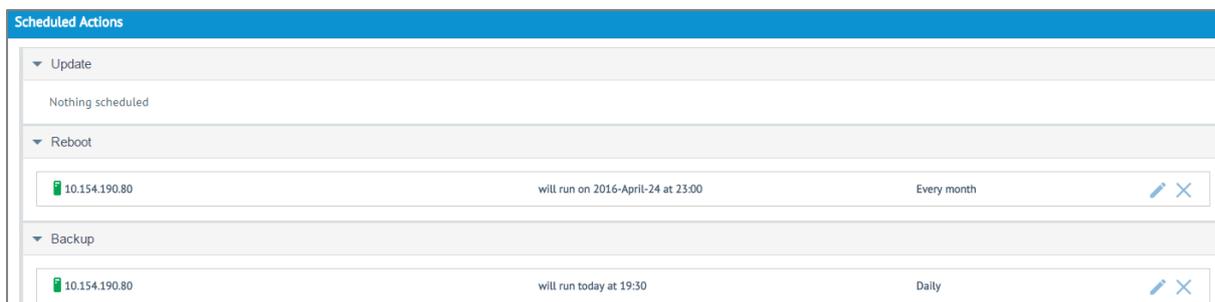


Figure 13-2: Scheduled Actions Screen

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

Set Schedule for LoadMaster

Schedule at 23 : 00 on 2016-April-24

Repeat Monthly

Cancel Schedule

Figure 13-3: Adjustable Schedule Settings

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

Tasks cannot be scheduled within one hour of each other.

13.3 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**.

Scheduled Actions

- Update
 - Nothing scheduled
- Reboot
 - 10.154.190.80 will run on 2016-April-24 at 23:00 Every month [cog] [x]
- Backup
 - 10.154.190.80 will run today at 19:30 Daily [cog] [x]

Figure 13-4: Scheduled Actions Screen

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

Delete Reboot Schedule 2016-April-24 at 23:00 on LoadMaster 10.154.190.80?

Are you sure you want to delete Reboot Schedule 2016-April-24 at 23:00 on LoadMaster 10.154.190.80 from the system?

Cancel Remove

Figure 13-5: Delete a Scheduled Action

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

14 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**.



Figure 14-1: Global Repository

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

14.1 System Logs

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

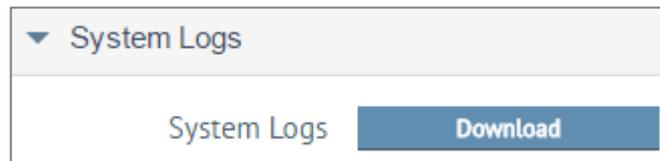


Figure 14-2: System Logs Download Button

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.

14.2 Diagnostic Logs

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

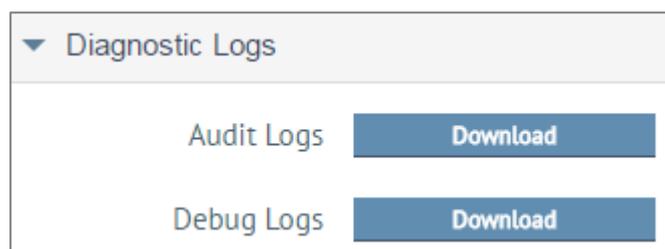


Figure 14-3: Diagnostic Logs Download Buttons

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.

14.3 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 **Section 7.4**.

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

15 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.

References

Related documents are listed below:

KEMP 360 Central API, Interface Description

KEMP 360 Central for Azure, Installation Guide

KEMP 360 Central Activation Server, Feature Description

Virtual Services and Templates, Feature Description

Web User Interface WUI, Configuration Guide

KEMP 360 Central Licensing, Feature Description

User Management, Feature Description

Health Checking, Feature Description

Metered Licensing Management, Feature Description

Document History

Date	Change	Reason for Change	Version	Resp.
Nov 2015	Initial draft	First draft of document	1.0	LB
Dec 2015	Additional Features	Release updates	2.0	KG
Jan 2016	Minor changes	Updates to Copyright Notices	3.0	LB
Jan 2016	Additional Features	Release Updates	4.0	KG
Feb 2016	Additional Features	Release Updates	5.0	KG
Apr 2016	Additional Features	Release Updates	6.0	KG
May 2016	Additional Features	Release Updates	7.0	KG
June 2016	Release updates	Updates for V1.6	8.0	LB
July 2016	Release updates	Updates for V1.7	9.0	LB
Aug 2016	Release updates	Updates for V1.8	10.0	LB
Sep 2016	Release updates	Updates for V1.9	11.0	LB
Oct 2016	Release Updates	Updates for V1.10	12.0	POC
Nov 2016	Release Updates	Updates for V1.11	13.0	POC
Jan 2017	Release Updates	Updates for V1.12	14.0	POC
Feb 2017	Release Updates	Enhancements made	15.0	POC
Feb 2017	Release updates	Updates for V1.13	16.0	POC
Mar 2017	Release updates	Updates for V1.14	17.0	POC