Multi-Tenant LoadMaster WUI

Configuration Guide

UPDATED: 17 October 2019

Copyright Notices

Table of Contents

1 Introduction

Multi-Tenant LoadMaster is Kemp's multi-tenancy product. It is a product where multiple independent instances of the Kemp LoadMaster and GEO LoadMaster can operate. These instances can be referred to as tenants or Virtual Network Functions (VNFs).

Each LoadMaster instance within Multi-Tenant LoadMaster can be deployed, stopped, started and updated at will.

1.1 Document Purpose

The purpose of this document is to describe the various options in the Multi-Tenant LoadMaster Web User Interface (WUI).

For a high-level overview of the Multi-Tenant LoadMaster product and architecture, refer to the **Kemp Multi-Tenant LoadMaster, Product Overview**.

For instructional steps on how to perform certain tasks in the Kemp Multi-Tenant LoadMaster, refer to the **Multi-Tenancy, Feature Description**.

1.2 Intended Audience

This document is intended to be read by anyone who is interested in learning about the features and functionality available in the Kemp Multi-Tenant LoadMaster product.

2 Multi-Tenancy Web User Interface (WUI) Options

The sections below describe the WUI options for the Multi-Tenant LoadMaster.

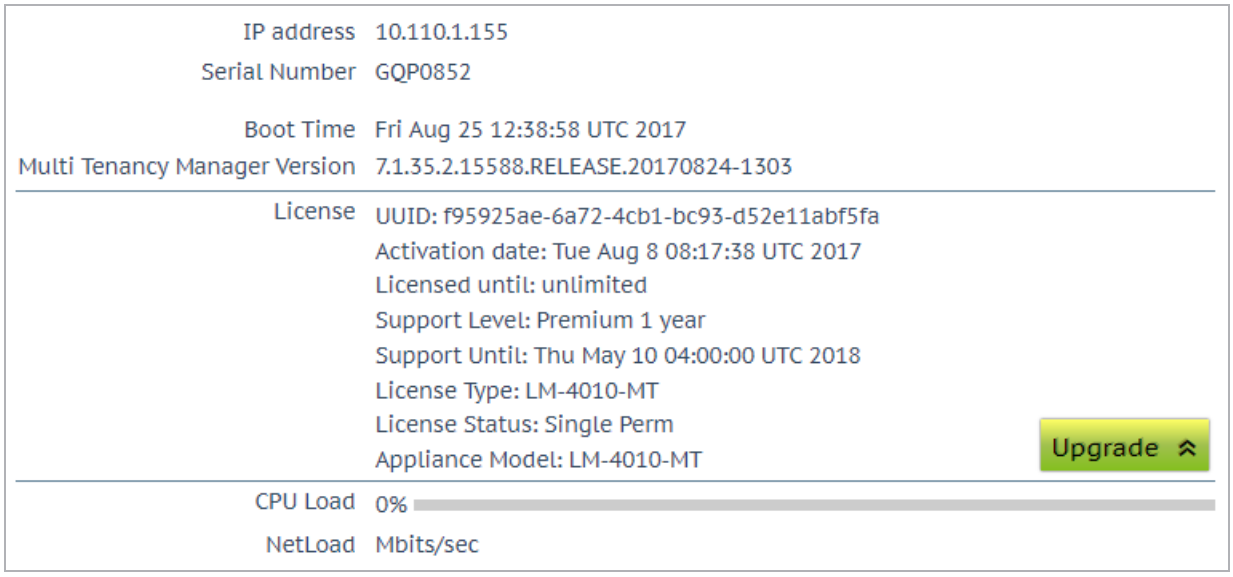
2.1 Initial VLM VNF Instantiation

After the Multi-Tenant LoadMaster installation is complete, and the password has been set, a prompt will appear asking if you would like to instantiate the first VLM VNF.

A check box will be displayed which specifies whether or not the MT guests should utilize DHCP for initial IP configuration. If this is enabled, the initial IP address and default gateway of the guest VNF will be automatically obtained using DHCP, and you will not be prompted to set them. If this option is disabled, text boxes will allow you to specify the initial IP address and default gateway.

There are also radio buttons which allow you to specify whether you would like to instantiate a VLM VNF now or not. If you select **Yes**, the **Create Instance** screen will appear and you will be prompted to configure the settings for the VNF. If you select **Not Right Now**, you will be brought to the Multi-Tenant LoadMaster home page.

2.2 Home



Clicking the **Home** menu option displays the home page which presents a list of basic information regarding the Multi-Tenant LoadMaster.

The following information is displayed on this screen:

IP address: The IP address of the Multi-Tenant LoadMaster

Serial Number: The serial number of the Multi-Tenant LoadMaster

Boot Time: The time of the last server reboot

Multi Tenancy Manager Version: The firmware version of the Multi-Tenant LoadMaster

License: License details are listed here, such as the activation date and end date of the Multi-Tenant LoadMaster license

CPU Load: The percentage of load to the CPU of the Multi-Tenant LoadMaster appliances

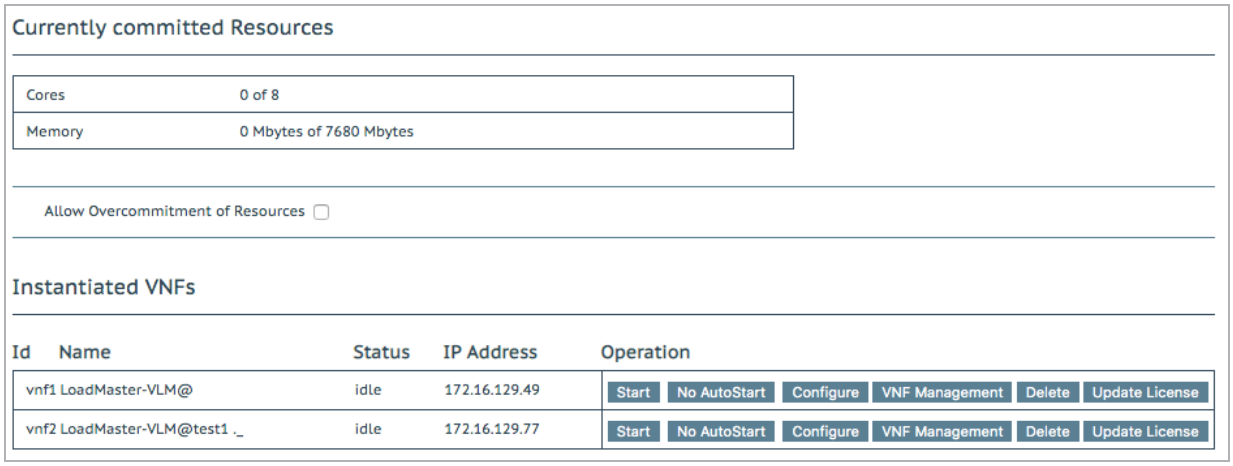
Net Load: The load of each configured interface. There are two bars shown for each interface - one represents the percentage of inbound traffic and the other represents the percentage of outbound traffic.

2.3 Instance Management

This section is where the administration of installed Virtual Network Functions (VNFs) occurs.

2.3.1 Virtual Network Functions (VNF) Status

This screen lists all the available VNFs and their status.



At the top of the screen the currently committed resources are displayed, that is, the number of cores in use and the amount of memory in use.

Allow Overcommitment of Resources

Selecting this check box allows resources to be overcommitted. This can have an impact on performance.

> By default, Multi-Tenant LoadMaster will only start running instances which do not exceed the total amount of available hardware resources.

A table is displayed which contains information and operations pertaining to each VNF. There are a number of columns in this table:

Id: A unique identifier for each VNF

Name: A name to distinguish the VNF

Status: Shows whether the VNF is idle or running

IP Address: The IPv4 or IPv6 address of the VNF. If the VNF is running, this will be displayed as a clickable hyperlink which will bring you to the VNF.

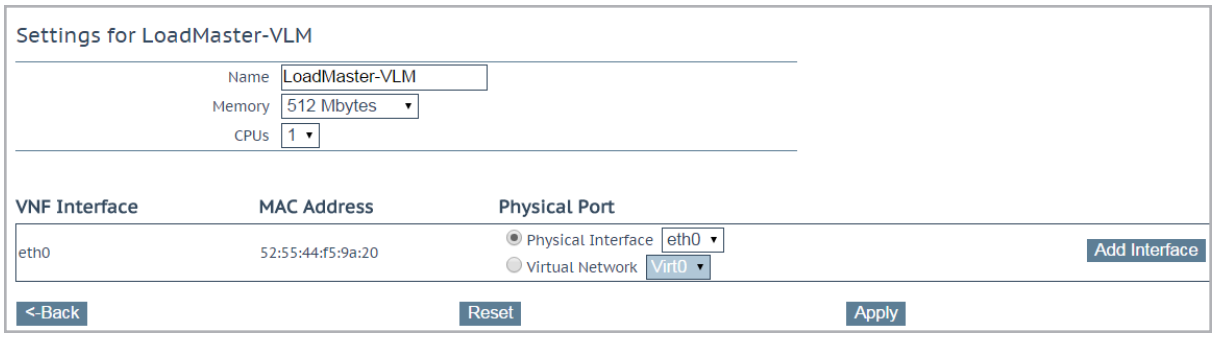
The last column contains a list of **Actions:**

- **Start/Stop:** Start/stop this VNF.

- **AutoStart/No AutoStart:** Specify whether the system should auto-start this VNF upon reboot or not.
- **Configure:** Modify the settings for this VNF, such as those relating to the memory, CPUs and IP addresses.
- **VNF Management:** Administer this VNF including deploying application templates.
- **Delete:** Delete this VNF. A VNF cannot be deleted if it is running. To delete a VNF, first stop the VNF, then click **Delete**.
- **Update License:** When the multi-tenant host license is updated, you can update the VNF license by clicking the **Update License** button. If the VNF is running, you must restart it to apply the new license.

2.3.1.1 Configure a VNF

The Multi-Tenant LoadMaster creates one Virtual-Switch per physical/VLAN interface. In addition, 10 host local networks are created. The tenant's vNICs connect either to one of these switches or to one of the host local networks. Each tenant can have up to 10 vNICs named **Virt0**-**Virt9**.



On this screen the VNF settings can be modified.

> The VNF has to be stopped to make changes on this screen. If the VNF has not been stopped, the fields on this screen will be greyed out. VNFs can be stopped on the **VNF Status** screen.

Name: The name of the VNF.

Memory: Select the amount of memory that is allocated to the VNF.

CPUs: Select the number of CPUs that have been allocated to the VNF.

> There is a limit to the VNF size of the maximum number of cores of a single CPU on a multi-core platform. For example, on a dual CPU system with six cores per CPU, the maximum size that can be configured for a single VNF is six cores.

The second half of this screen lists the interfaces for this VNF along with related operations.

VNF Interface: The interface number.

MAC Address: The Media Access Control (MAC) address of the VNF.

Physical Interface/Virtual Network: To select either a physical interface or virtual network and select the relevant interface.

Add Interface: Adds the interface.

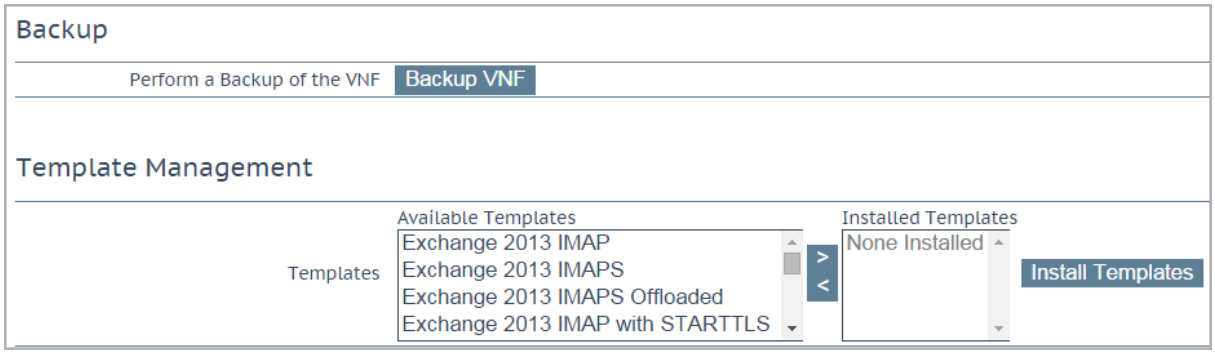
Delete Interface: Deletes the interface.

> The interfaces can only be configured when the VNF is not running.

Reset: Resets all values to the default settings.

Apply: Applies the changes to the VNFs.

2.3.1.2 Manage a VNF



Administrative functions can be performed to VNFs on this screen.

Backup VNF

Take a backup of the VNF.

> The backup name includes a date and timestamp. This has a granularity of one minute. If more than one backup is created in the same minute, the original backup (with the same name) will be overwritten. If there is more than one minute between backup attempts, a separate file will be created.

Available Backups

Shows a list of previous backups for this VNF (if any exist).

Restore: Restore the backup to the VNF.

Download: Downloads the backup to the local machine.

Delete: Deletes the backup.

Templates

A list of available Virtual Service templates is displayed on the left. Templates can be moved to the **Installed Templates** list on the right by selecting them and clicking the right arrow. To remove templates, use the left arrow. Click **Install Templates** to apply the changes to the VNF.

2.3.2 Package Management

Import VNF Package

Import a new VNF package.

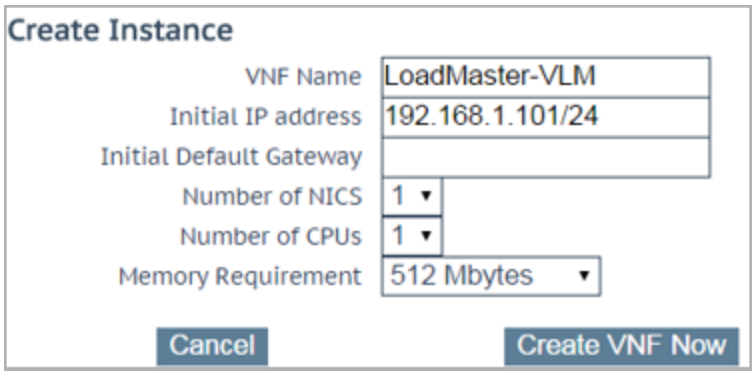
Package: The name of the VNF package.

Version: The VNF package version.

Operation:

- **Create Instance:** Create an instance of this VNF.
- **Delete:** Delete this VNF template.

2.3.2.1 Create a VNF Instance



VNF Name: Specify the name of the VNF.

Initial IP address: Enter the initial IP address of the VNF.

Initial Default Gateway: Enter the initial default gateway of the VNF.

> If the **Enable DHCP for MT VNF(s)** option is enabled (**System Configuration > Miscellaneous Options > Network Options**), the **Initial IP address** and **Initial Default Gateway** fields will not be displayed because the initial IP address and default gateway will be automatically obtained via DHCP.

Number of NICS: Select the number of Network Interface Console (NICs).

Number of CPUs: Select the number of CPUs that are required for this VNF.

> There is a limit to the VNF size of the maximum number of cores of a single CPU on a multi-core platform. For example, on a dual CPU system with six cores per CPU, the maximum size that can be configured for a single VNF is six cores.

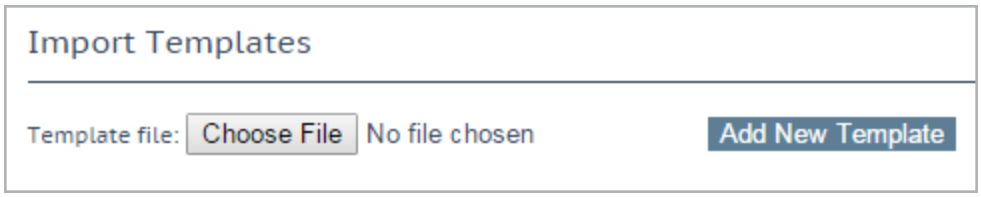
Memory Requirement: Select the amount of memory allowed for this VNF.

Create VNF Now: Creates an instance of this VNF.

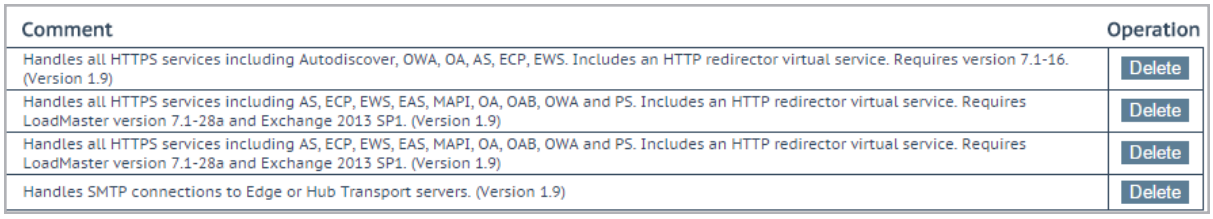
2.3.3 Manage Templates

Application templates make the setting up of Virtual Services easier by automatically configuring the parameters for a Virtual Service. Before a template can be used to configure a Virtual Service, it must be imported and installed on the Multi-Tenant LoadMaster or a tenant LoadMaster.

Templates can be downloaded from www.kemptechnologies.com.



Click the **Choose File** button, select the template you wish to install and click the **Add New Template** button to install the selected template. This template then needs to be assigned to the VNF in the **Manage VNF** screen before it becomes available for use in the tenant LoadMaster. Refer to the **Manage a VNF** section for more information.

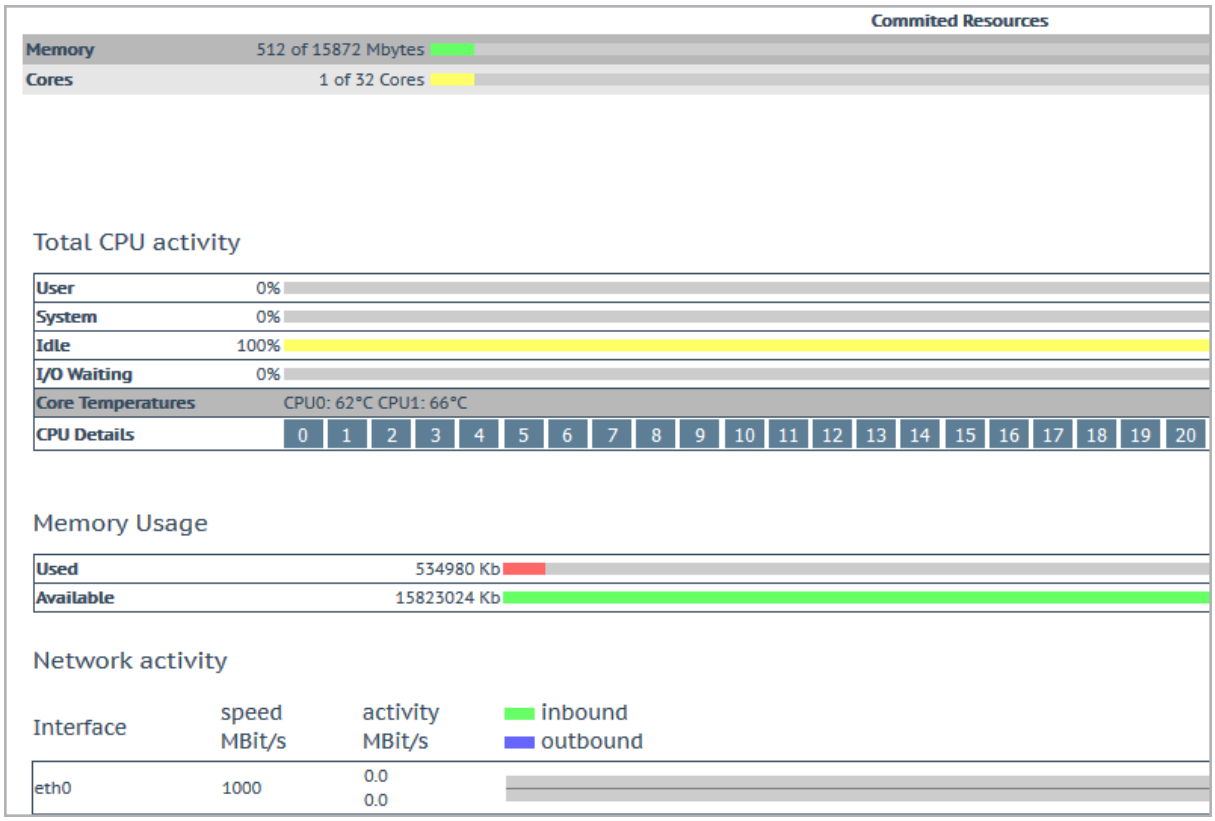


Click the **Delete** button to remove the template.

For details on how to use a template to create and configure a new Virtual Service and where to obtain templates, please refer to the **Virtual Services and Templates, Feature Description** document.

2.4 Statistics

2.4.1 Real Time Statistics



The **Statistics** screen displays the activity and resources used of the Multi-Tenant LoadMaster.

2.4.1.1 Committed Resources

Memory: The amount of total memory used for the committed resources. This relates to the VNFs.

Cores: The number of processor cores in use.

> There is a limit to the VNF size of the maximum number of cores of a single CPU on a multi-core platform. For example, on a dual CPU system with six cores per CPU, the maximum size that can be configured for a single VNF is six cores.

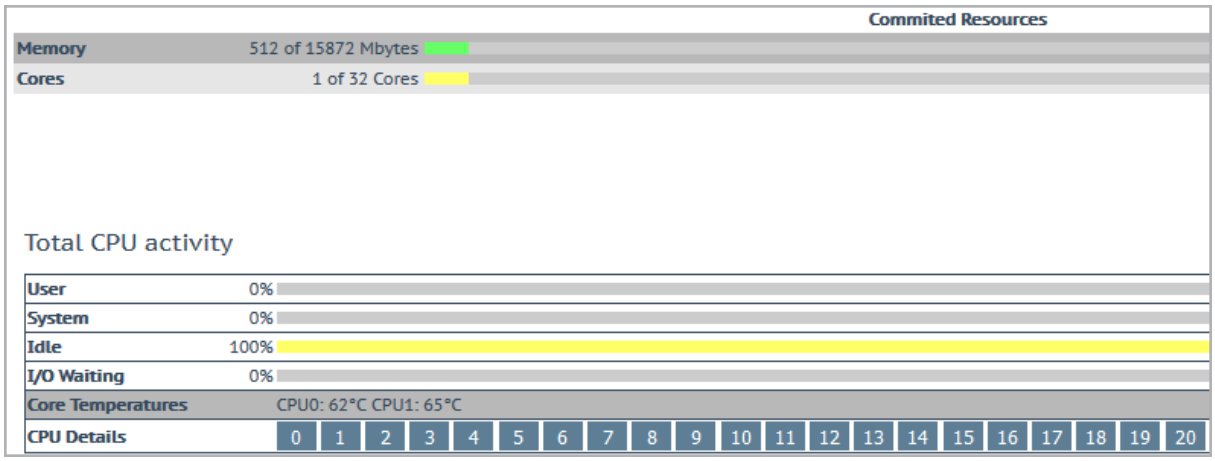
2.4.1.2 Total CPU activity

This table displays the following CPU utilization information for a given Multi-Tenant LoadMaster:

Statistic	Description
User	The percentage of the CPU spent processing in user mode
System	The percentage of the CPU spent processing in system mode
Idle	The percentage of CPU which is idle
I/O Waiting	The percentage of the CPU spent waiting for I/O to complete

The sum of these 4 percentages will equal 100%.

Core Temp: The temperature for each CPU core is displayed for Multi-Tenant LoadMaster hardware appliances. Temperature will not show on a virtual statistics screen.



CPU Details: The number buttons can be clicked in the **CPU Details** row to get more detailed statistics on each CPU, as shown in the screenshot above.

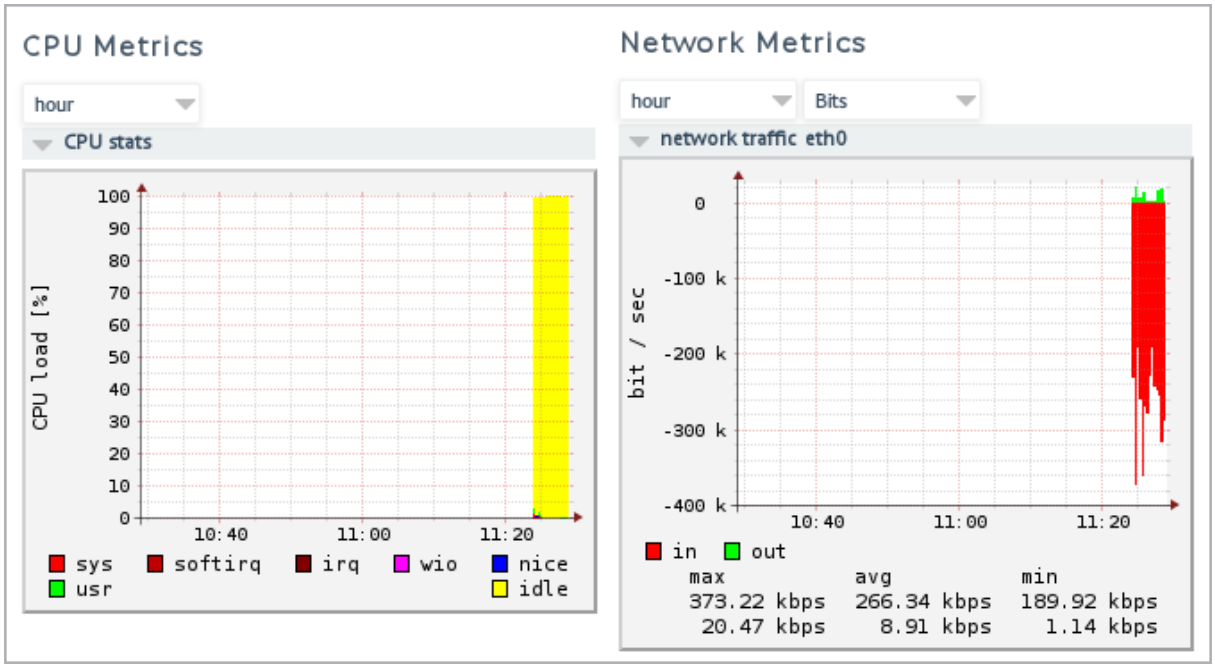
Memory usage

This bar graph shows the amount of memory in use and the amount of memory free for the host Multi-Tenant LoadMaster system.

Network activity

These bar graphs show the current network throughput on each interface.

2.4.2 Historical Graphs



The **Historical Graphs** screen provides a graphical representation of the Multi-Tenant LoadMaster statistics. These configurable graphs provide a visual indication of the traffic that is being processed by the Multi-Tenant LoadMaster.

There are graphs for the network activity on each interface. The time granularity can be specified by selecting one of the **hour, day, month, quarter** or **year** options.

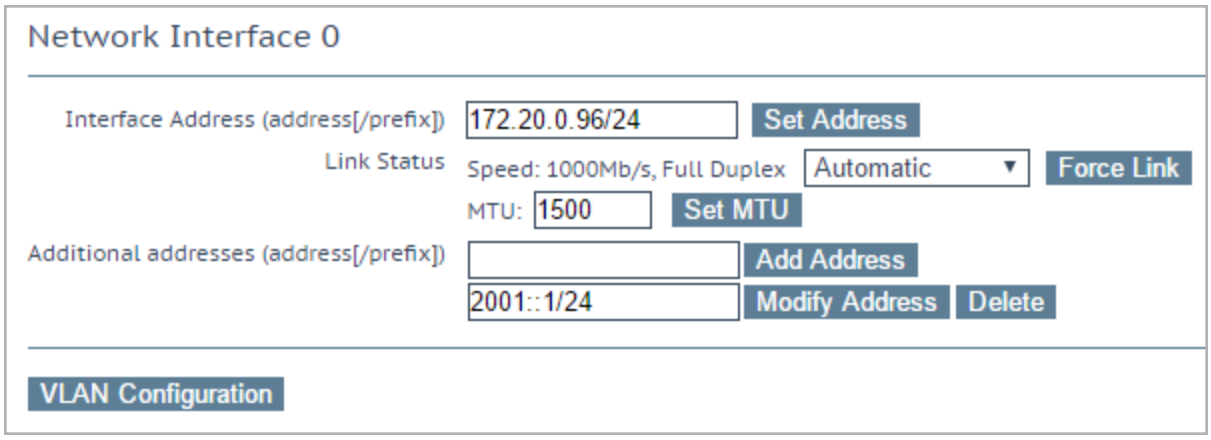
In the case of the network activity on the interface graphs, you can choose which type of measurement unit you wish to use by selecting one of the **Packet, Bits** or **Bytes** options.

You can disable these graphs by disabling the **Enable Historical Graphs** check box in the **WUI Settings** screen. For more information on the **WUI Settings** section, refer to the **WUI Settings** section.

2.5 System Configuration

2.5.1 Interfaces

Describes the external network and internal network interfaces. The screen has the same information for all Ethernet ports.



Within the **Interface Address (address[/prefix])** text box you can specify the Internet address of this interface.

By default, the **Speed** of the link is automatically detected. In certain configurations, this speed is incorrect and must be forced to a specific value.

> The interface speed displayed for VNF virtual interfaces within the VNF user interface is always 1000 Mb/s; the speed set on the corresponding MT physical interface (if any) is irrelevant.

The **Use for Default Gateway** check box is only available if the **Enable Alternate GW support** is selected in the **Network Options** screen. If the settings being viewed are for the default interface this option will be grayed out and selected. To enable this option on another interface, go to the other interface by clicking it in the main menu on the left. Then this option is available to select.

Within the **MTU** field you can specify the maximum size of Ethernet frames that will be sent from this interface. The valid range is **512** - **9216**.

> The valid range of **512** - **9216** may not apply to VLMs as the range will be dependent on the hardware the VLM is running on. It is advised to check your hardware restrictions for supported MTU sizes.

Using the **Additional addresses** field allows the Multi-Tenant LoadMaster to give multiple addresses to each interface, as aliases. This is sometimes referred to as a “router on a stick”. It allows both IPv4 and IPv6 addresses in standard IP+CIDR format, so this can also be used to do a mixed mode of IPv4 and IPv6 addresses on the same interface. Any of the subnets that are added here will be available for both virtual IPs and real server IPs.

Creating a Bond/Team

Before creating a bonded interface please note the following:

- You can only bond interfaces higher than the parent, so if you choose to start with eth1, you can then bond eth2, eth3 and above, but you cannot bond eth0 (unless you start with eth0)
- Bond links first if you need VLAN tagging then add VLANs after the bond has been configured
- To add a link to a bonded interface, any IP addressing must first be removed from the link to be added
- Enabling the Active-Backup mode generally does not require switch intervention
- Bonding **eth0** with **eth1** can lead to serious issues and is not allowed to occur

Click **Interface Bonding** to request the bond.

Confirm the bond creation by clicking **Create a bonded interface**.

Acknowledge the warning dialogs.

Using the Web User Interface (WUI) select the **System Configuration > Interfaces > bndx** menu option.

If you do not see the **bndX** interface, refresh your browser, then select the bonded interface and click the **Bonded Devices** button.

Select the desired bonding mode.

Add the additional interfaces to this bond.

Configure the IP and Subnet Mask on the bonded interface.

Removing a Bond/Team

Remove all VLANs on the bonded interface first; if you do not remove them they will automatically be assigned to the physical port at which the bond started.

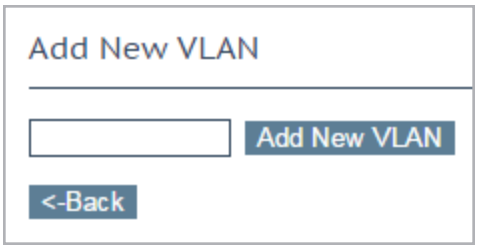
Select the **System Configuration > Interfaces > bndx** menu option. If you do not see the **bndX** interface refresh your browser, then select the bonded interface, then click the **Bonded Devices** button.

Unbind each port by clicking **Unbind Port**, repeat until all ports have been removed from bond.

Once all child ports have been unbounded, you can unbond the parent port by clicking **Unbond this interface** button.

Adding a VLAN

Select the interface and then select the **VLAN Configuration** button.



Add the **VLAN Id** value and select the **Add New VLAN** menu option.

Repeat as needed. To view the VLANs, select the **System Configuration > Interfaces** menu option.

Removing a VLAN

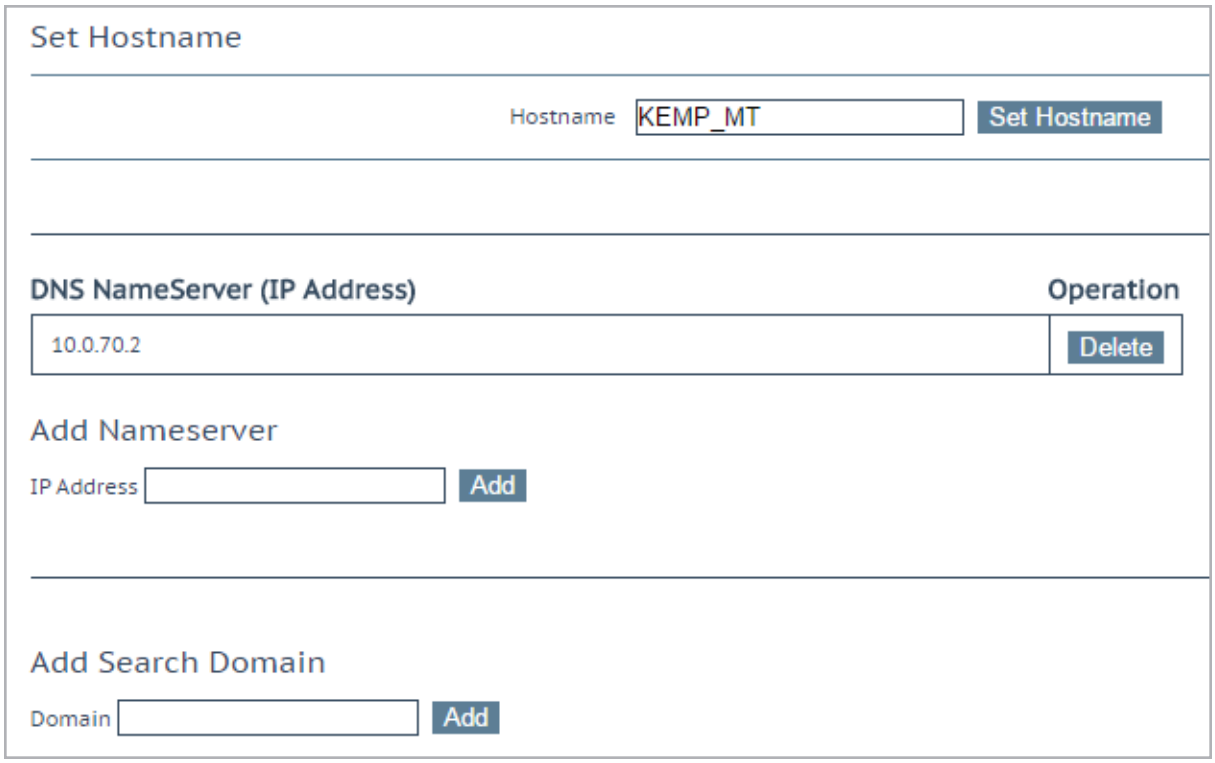
To remove a VLAN select the **System Configuration > Interfaces** menu option and select the appropriate VLAN ID from the drop-down list.

Once selected, delete the IP and then click **Set Address**. Once the IP has been removed you will have the option to delete the VLAN, by clicking the **Delete this VLAN** button.

Repeat as needed. To view the VLANs select the **System Configuration > Interfaces** menu option and select the appropriate VLAN ID from the drop-down list.

2.5.2 Host & DNS Configuration

2.5.2.1 Hostname Configuration



Set Hostname

Set the hostname of the local machine by entering the hostname in the **Current Hostname** text box and clicking the **Set Hostname** button. Only alphanumeric characters are allowed.

DNS NameServer (IP Address)

Enter the IP address of a DNS server that will be used to resolve names locally on the Multi-Tenant LoadMaster in this field and click the **Add** button. A maximum of three DNS servers are allowed.

DNS Search Domains

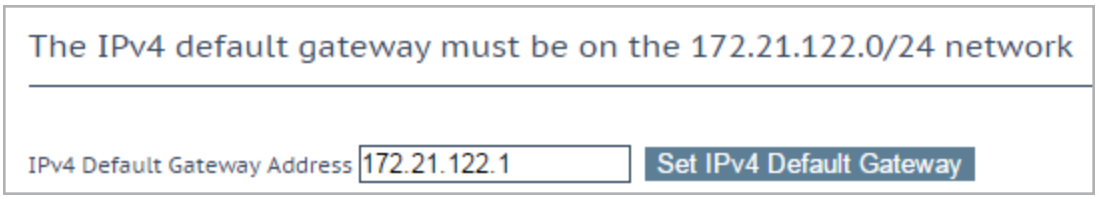
Specify the domain name that is to be prepended to requests to the DNS Name Server in this field and click the **Add** button. A maximum of six Search Domains are allowed.

2.5.3 Route Management

This option permits the configuration of default and static routes.

2.5.3.1 Default Gateway

The LoadMaster requires a default gateway through which it can communicate with the Internet.



If both IPv4 and IPv6 addresses are being used on the Multi-Tenant LoadMaster, then both an IPv4 and IPv6 Default Gateway Address are required.

> IPv4 and IPv6 default gateways must be on the same interface.

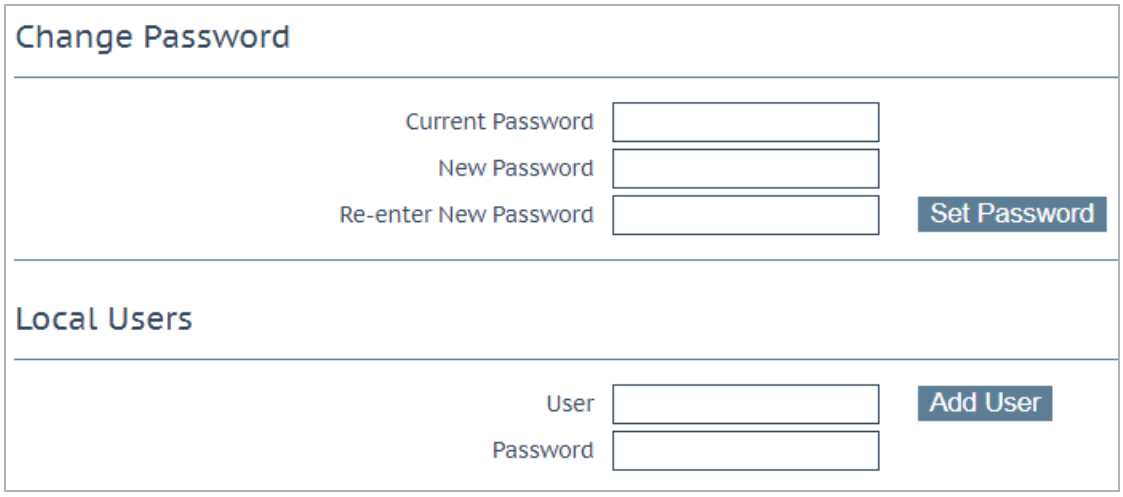
2.5.3.2 Additional Routes

Further routes can be added. These routes are static and the gateways must be on the same network as the Multi-Tenant LoadMaster.

2.5.4 System Administration

These options control the base-level operation of the Multi-Tenant LoadMaster. Many of these options will require a system reboot.

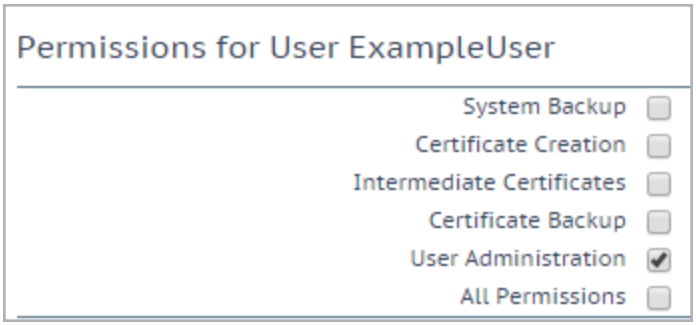
2.5.4.1 User Management



The User Management screen allows you to:

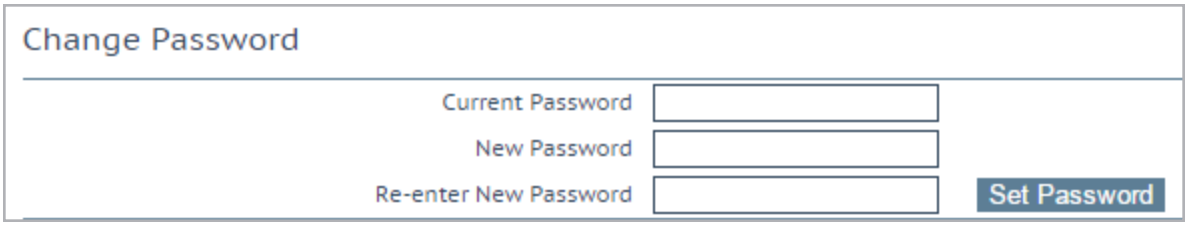
- Change the appliance password
- Change an existing user's password by clicking the **Password** button in the **Action** section
- Add a new user and associated password
- Change the permissions for an existing user by clicking the **Modify** button in the **Action** section

User names can contain alphanumeric characters and periods and dashes ('.' and '_').



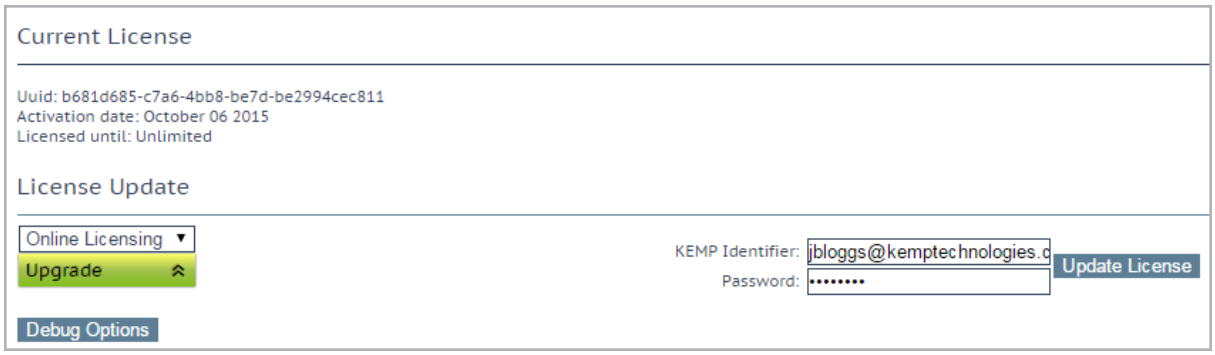
In this screen you may set the level of user permissions. This determines what configuration changes the user is allowed to perform. The primary user, bal, always has full permissions. Secondary users may be restricted to certain functions.

Named users, even those without User Administration privileges, can change their own passwords. When a named user clicks the **System Administration > User Management** menu option the **Change Password** screen appears.



From within this screen, users can change their own password. Once changed, a confirmation screen appears after which the users will be forced to log back in to Multi-Tenant LoadMaster using their new password.

2.5.5 Update License



This screen displays the activation date and the expiration date of the current license. You would use the **Update License** function if your license has changed, for example if:

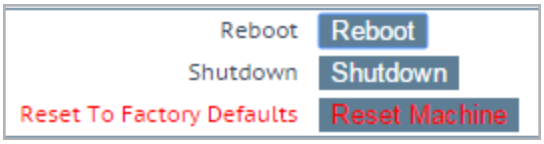
- You have renewed support
- You have renewed your license
- You have changed your license type

Before updating the license in the Multi-Tenant LoadMaster, you must either contact your Kemp representative or use the **Upgrade** option (to update your license). After you have contacted Kemp or used the **Upgrade** option, there are two ways to upgrade a license – using the Online method and using the Offline method. For more information and instructions, refer to the **Licensing, Feature Description**. A reboot is recommended after updating the license.

Licensing is done in the Multi-Tenant LoadMaster and is based on the maximum number of tenants that can be started. This means that the LoadMaster tenants do not need to be licensed individually. 10 is the maximum number of tenants for the default Multi-Tenant LoadMaster license.

To update the license of an individual VNF, first update the license on the Multi-Tenant LoadMaster, then click the **Update License** button for the relevant VNF on the **VNF Status** screen. If the VNF is running, you must restart it to apply the new license. To restart a VNF, go to **Instance Management > Virtual Network Functions (VNF) Status**, click **Stop** on the relevant VNF and then click **Start** to restart it.

2.5.6 System Reboot



Reboot

Reboot the appliance.

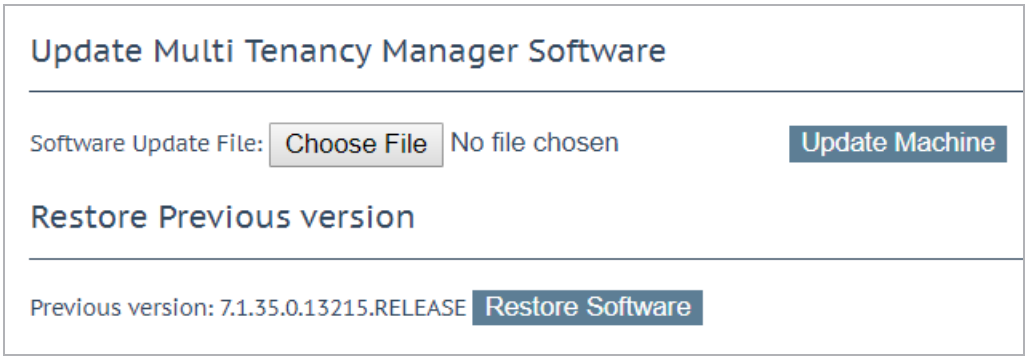
Shutdown

Clicking this button attempts to power down the Multi-Tenant LoadMaster.

Reset Machine

Reset the configuration of the appliance with the exception of the license and username and password information.

2.5.7 Update Software



Contact support to obtain the location of firmware patches and upgrades. Firmware downloads require Internet access. Detailed patch information is available at https://support.kemptechnologies.com (search for LoadMaster MT Release Notice).

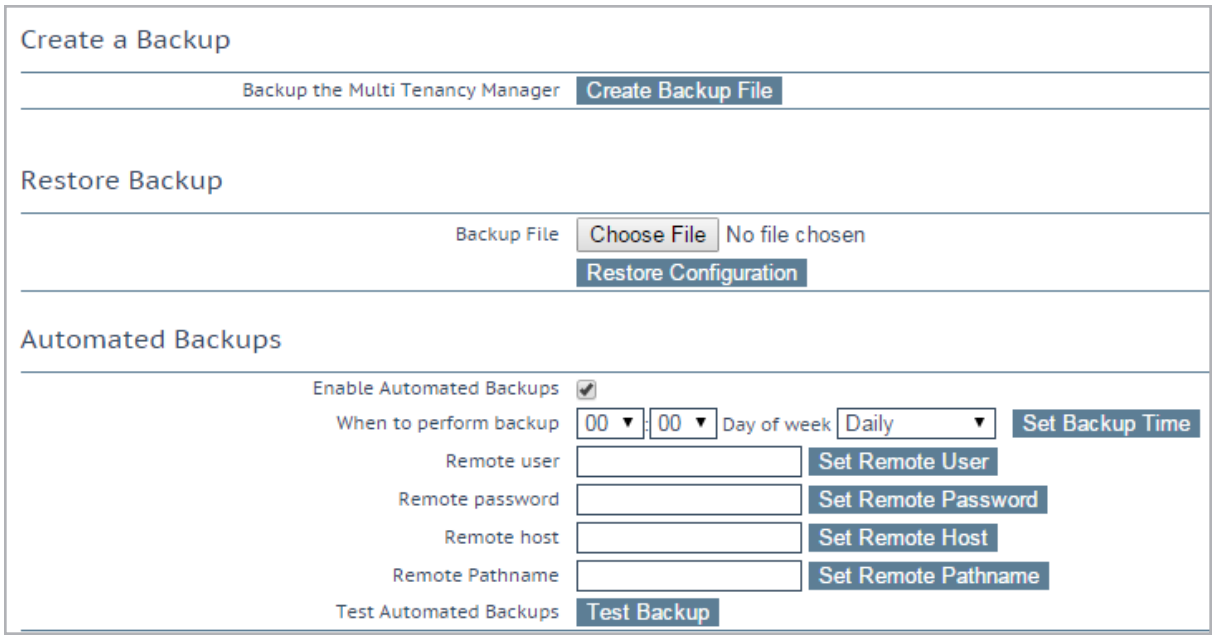
Update Machine

Once you have downloaded the firmware you can browse to the file and upload the firmware directly into the Multi-Tenant LoadMaster. The firmware will be unpacked and validated on the Multi-Tenant LoadMaster. If the patch is validated successfully you will be ask to confirm the release information. To complete the update you will need to reboot the appliance. This reboot can be deferred if needed.

Restore Software

If you have completed an update of the Multi-Tenant LoadMaster firmware you can use this option to revert to the previous build.

2.5.8 Backup and Restore



Create Backup File

Generate a backup of the Multi-Tenant LoadMaster. License information is not contained in the backup.

Restore Configuration

Browse to and restore a Multi-Tenant LoadMaster backup file.

Automated Backups

If the **Enable Automated Backups** check box is selected, the system may be configured to perform automated backups on a daily or weekly basis.

When to perform backup

Specify the time (24 hour clock) of backup. Also select whether to backup daily or on a specific day of the week. When ready, click the **Set Backup Time** button.

Remote user

Set the username required to access remote host.

Remote password

Set the password required to access remote host.

Remote host

Set the remote host name.

Remote Pathname

Set the location on the remote host to store the file.

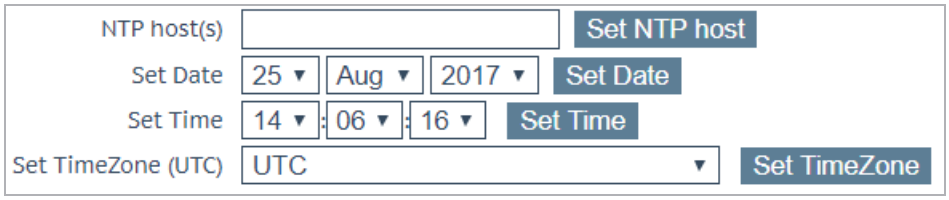
Test Automated Backups

Clicking the **Test Backup** button performs a test to check if the automated backup configuration is working correctly. The results of the test can be viewed within the System Message File.

> The Automated Backup transfer protocol is currently FTP only.

2.5.9 Date/Time

You can manually configure the date and time of the Multi-Tenant LoadMaster or leverage a Network Time Protocol (NTP) server.



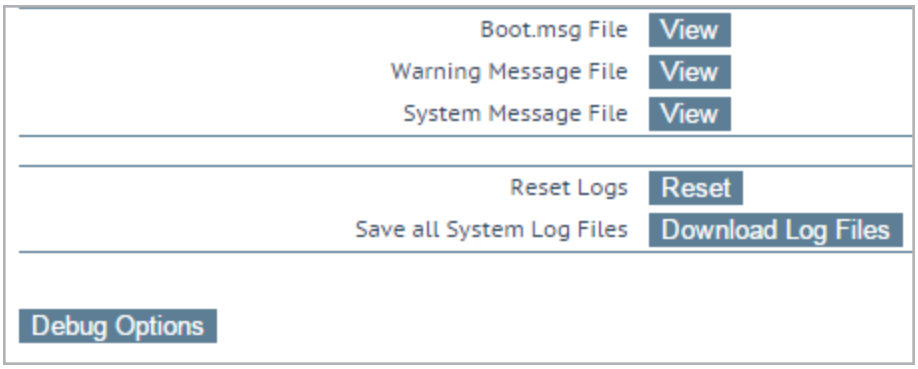
NTP host(s)

Specify the host which is to be used as the NTP server. Multiple hosts can be entered by using a space-separated list.

> The time zone must always be set manually.

2.5.10 Logging Options

2.5.10.1 System Log Files



Boot.msg File: Contains information, including the current version, during the initial starting of the Multi-Tenant LoadMaster.

Warning Message File: Contains warnings logged during the operation of the Multi-Tenant LoadMaster.

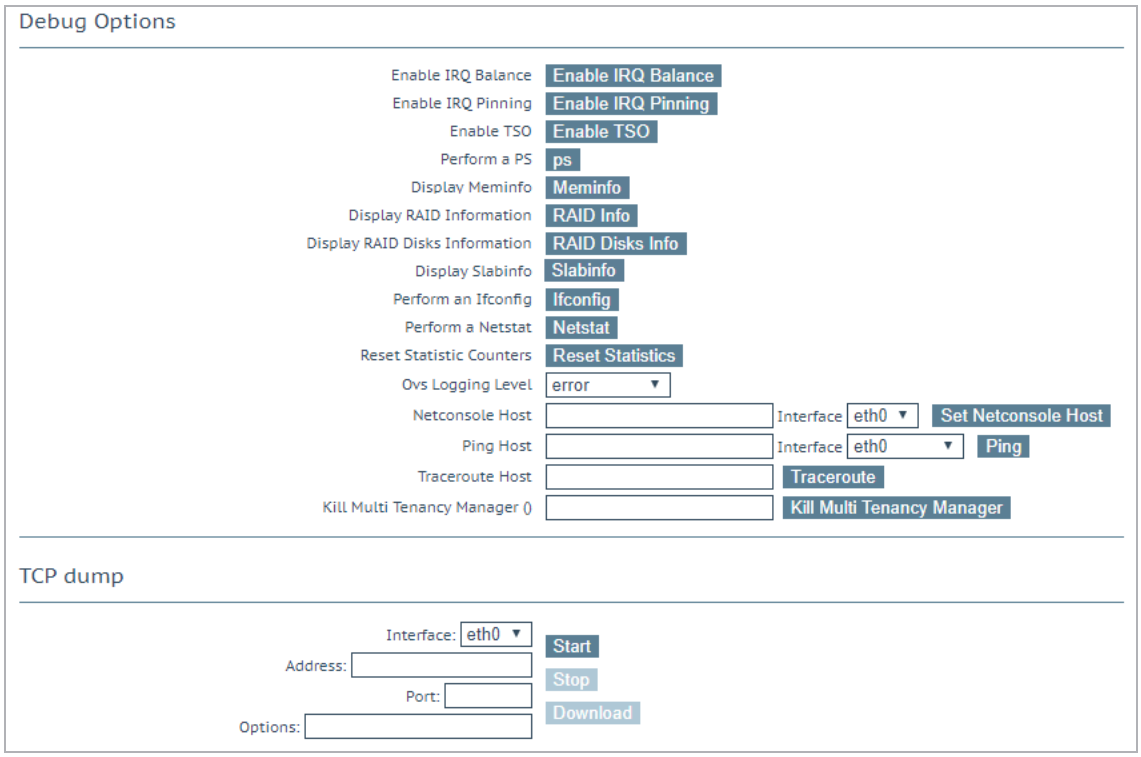
System Message File: Contains system events logged during the operation of Multi-Tenant LoadMaster. This includes both operating system-level and Multi-Tenant LoadMaster internal events.

Reset Logs: This will reset all log files.

Save all System Log Files: This saves the files to your computer. It can be useful to send log files to Kemp support when troubleshooting an issue.

2.5.10.1.1 Debug Options

The Multi-Tenant LoadMaster has a range of features that will help you and Kemp Support staff with diagnosing connectivity issues. Clicking the **Debug Options** button will bring up the screen shown below.



Enable IRQ Balance: Enable this option only after consulting with Kemp support staff.

Perform a PS: Performs a ps on the system.

Display Meminfo: Displays raw memory statistics.

Display RAID Information

> The **Display RAID Information** and **Display RAID Disks Information** buttons only appear if a RAID controller is installed on the Multi-Tenant LoadMaster host.

Display the Redundant Array of Independent Disks (RAID) controller details. Some example information is below:

```
-----------------------------------------------------------------
Controller details
-----------------------------------------------------------------
- Chip ID.................: 10
- Parent Controller Index: 255
- OS Physical Name.......: /dev/sda
- Serial Number..........: 427491329
```



```
- AES Power on State.....: 0
- Sata Ports.............: 2
-----------------------------------------------------------------
Raid Port 0 details
-----------------------------------------------------------------
- Raid Model Name............: H/W RAID1
- Raid Serial Number.........: OUEYEXCXTQ53GE1BSOSN
- EZBackup Disk Support......: 0
- Port Multiplier port.......: 0
- Raid Capacity..............: 953 (29 GB)
- Raid Capacity low word.....: 0
- Raid State.................: 1 (Active)
- Raid Status................: 3 (Normal)
- Raid Level.................: 1 (Raid 1 (mirror))
- Mark Type..................: 0
- Active Member..............: 15
- Active Level...............: 0
- Rebuild Priority...........: 3
- Standby Timer..............: 0
- Total members in the RAID....: 2
Member disk 0
- Ready.....................: 1
- Lba 48 Bit Support.......: 1
- SATA Page.................: 0
- SATA Port.................: 0
- SATA Base.................: 0
- SATA Size.................: 953
-----------------------------------------------------------
Member disk 1
- Ready.....................: 1
- Lba 48 Bit Support.......: 1
- SATA Page.................: 0
- SATA Port.................: 1
- SATA Base.................: 0
- SATA Size.................: 953
-----------------------------------------------------------
```


Display RAID Disks Information

Display details about the RAID disks. Some example information is below:

```
-----------------------------------------------------------------
Sata Port 0 details
-----------------------------------------------------------------
- Disk Model Name..............: 32GB SATA Flash Drive
- Disk Serial Number...........: C0122916B01000000074
- Disk Firmware Version........: SFDC001D
- EZBackup Disk Support........: 1
- Port Multiplier port.........: 15
- Disk Capacity................: 954 (29 GB)
- Port Type....................: 2 (RAID)
- Port Speed...................: 2 (GB)
- Page 0 State.................: 2
- Page 0 Raid Index............: 0
- Page 0 Member Index..........: 0
- Page 0 Raid Name.............:
- Page 0 Raid Serial Number....:
- Page 0 Raid Segment Base.....: 0
- Page 0 Raid Size.............: 953
- Page 0 Raid EZ Backup Support: 0
- Page 1 State.................: 0
- Page 1 Raid Index............: 0
- Page 1 MemberIndex...........: 0
- Page 1 Raid Name.............:
- Page 1 Raid Serial Number....:
- Page 1 Raid Segment Base.....: 0
- Page 1 Raid Size.............: 0
- Page 1 Raid EZ Backup Support: 0
- PortErrorStatus..............: 0
-----------------------------------------------------------------
Sata Port 1 details
-----------------------------------------------------------------
- Disk Model Name..............: 32GB SATA Flash Drive
- Disk Serial Number...........: E011321290100000005A
- Disk Firmware Version........: SFDC001D
```

```
- EZBackup Disk Support........: 1
- Port Multiplier port.........: 15
- Disk Capacity................: 954 (29 GB)
- Port Type....................: 2 (RAID)
- Port Speed...................: 2 (GB)
- Page 0 State.................: 2
- Page 0 Raid Index............: 0
- Page 0 Member Index..........: 1
- Page 0 Raid Name.............:
- Page 0 Raid Serial Number....:
- Page 0 Raid Segment Base.....: 0
- Page 0 Raid Size.............: 953
- Page 0 Raid EZ Backup Support: 0
- Page 1 State.................: 0
- Page 1 Raid Index............: 0
- Page 1 MemberIndex...........: 0
- Page 1 Raid Name.............:
- Page 1 Raid Serial Number....:
- Page 1 Raid Segment Base.....: 0
- Page 1 Raid Size.............: 0
- Page 1 Raid EZ Backup Support: 0
- PortErrorStatus..............: 0
```

Display Slabinfo: Displays raw slab statistics.

Perform an Ifconfig: Displays raw Ifconfig output.

Perform a Netstat: Displays Netstat output.

Reset Statistic Counters: Reset all statistic counters.

Ovs Logging Level: Specify the level of Open vSwitch logs to record. The default setting for this field is **error**.

Netconsole Host: The syslog daemon on the specified host will receive all critical kernel messages. The syslog server must be on the local LAN and the messages sent are UDP messages.

You can select which interface the Netconsole Host is set to using the **Interface** dropdown.

> Please ensure that the netconsole host specified is on the selected interface as errors may occur if it is not.

Ping Host: Performs a ping on the specified host. The interface which the ping should be sent from can be specified in the **Interface** drop-down list. The **Automatic** option selects the correct interface to ping an address on a particular network.

Traceroute Host: Perform a traceroute of a specific host.

Kill MT Console (): Permanently disables all Multi-Tenant LoadMaster functions. The Multi-Tenant LoadMaster can be re-enabled by being relicensed.

> Please do not kill your Multi-Tenant LoadMaster without consulting Kemp Technical Support first.

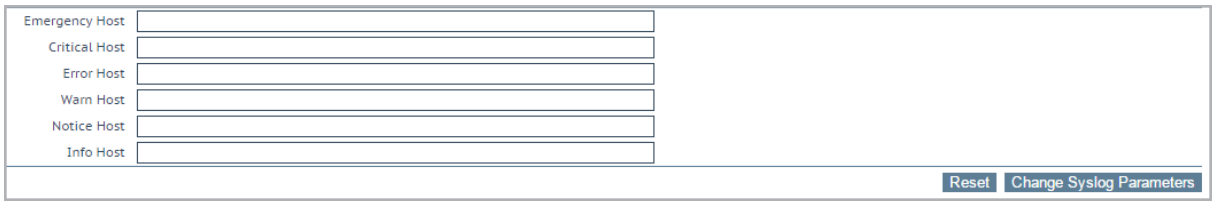
TCP dump

A TCP dump can be captured either by one or all Ethernet ports. Address and port parameters, as well as optional parameters may be specified. The maximum number of characters permitted in the optional field is **255**.

You can stop and start the dump. You can also download it to a particular location.

2.5.10.2 Syslog Options

The Multi-Tenant LoadMaster can produce various warning and error messages using the syslog protocol. These messages are normally stored locally.



It is also possible to configure the Multi-Tenant LoadMaster to transmit these error messages to a remote syslog server by entering the relevant IP address in the relevant text box and clicking **Change Syslog Parameters**.

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.

Examples of the type of message that may be seen after setting up a Syslog server are below:

- **Emergency**: Kernel-critical error messages

- **Critical**: Unit has failed
- **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

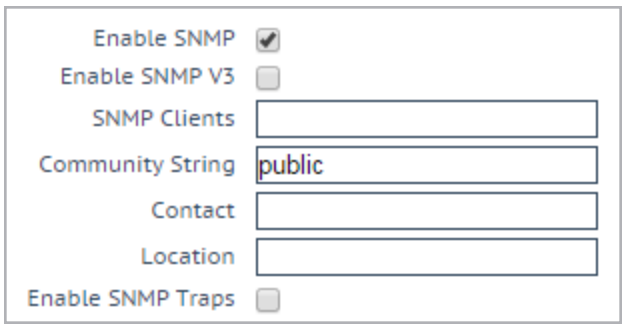
> One point to note about syslog messages is they are cascading in an upwards direction. Thus, if a host is set to receive WARN messages, the message file will include message from all levels above WARN but none for levels below WARN.

We recommend you do not set all six levels for the same host because multiple messages for the same error will be sent to the same host.

To enable a syslog process on a remote Linux server to receive syslog messages from the Multi-Tenant LoadMaster, the syslog must be started with the "-r" flag.

2.5.10.3 SNMP Options

With this menu, the SNMP configuration can be modified.



Enable SNMP

This check box enables or disables SNMP metrics. For example, this option allows the Multi-Tenant LoadMaster to respond to SNMP requests.

By default SNMP is disabled.

When the feature is enabled, the following traps are generated:

- **ColdStart**: generic (start/stop of SNMP sub-system)
- **VsStateChange**: (Virtual Service state change)

- **RsStateChange:** (Real Server state change)

The information regarding all Multi-Tenant LoadMaster-specific data objects is stored in three enterprise-specific MIBs (Management Information Base).

ONE4NET-MIB.txt	enterprise id
IPVS-MIB.txt	Virtual Server stats
B-100-MIB.txt	Multi-Tenant LoadMaster configuration data

These MIBs (which can be found on the Kemp website) need to be installed on the SNMP manager machine in order to be able to request the performance-/config-data of the Multi-Tenant LoadMaster using SNMP.

The description of the counters can be taken from the Multi-Tenant LoadMaster MIBs (the description clause). Apart from just reading the MIB this can be done for Linux (nad ucdsnmp) with the command:

snmptranslate -Td -OS <oid>

where <oid> is the object identifier in question.

Example: <oid> = .1.3.6.1.4.1.one4net.ipvs.ipvsRSTable.rsEntry.RSConns

snmptranslate -Td –Ov
.1.3.6.1.4.1.one4net.ipvs.ipvsRSTable.rsEntry.RSConns.1.3.6.1.4.1.12196.12.2.1.12

RSConns OBJECT-TYPE

-- FROM IPVS-MIB

SYNTAXCounter32

MAX-ACCESSead-only

STATUScurrent

DESCRIPTION"the total number of connections for this RS"

::= { iso(1) org(3) dod(6) internet(1) private(4) enterprises(1) one4net(12196) ipvs(12) ipvsRSTable(2) rsEntry(1) 12 }

The data object defined in the Multi-Tenant LoadMaster MIBS is a superset to the counters displayed by the WUI.

> The data objects on the Multi-Tenant LoadMaster are not writable, so only GET requests (GET, GET-NEXT, GET-BULK, and so on) should be used.

Enable SNMP V3

This check box enables SNMP v3 metrics. SNMPv3 primarily added security and remote configuration enhancements to SNMP.

When this option is enabled, two additional fields become available - **Username** and **Password**.

> The **Username** and **Password** must be set in order for SNMP v3 to work.

> The password must be at least 8 characters long.

Authentication protocol

Select the relevant **Authentication protocol** - **MD5** or **SHA**. **SHA** is a more secure protocol.

Privacy protocol

Select the relevant **Privacy protocol** - **AES** or **DES**. **AES** is a more secure protocol.

SNMP Clients

With this option, the user can specify from which SNMP management hosts the Multi-Tenant LoadMaster will respond to.

> If no client has been specified, the Multi-Tenant LoadMaster will respond to SNMP management requests from any host.

SNMP Community String

This option allows the SNMP community string to be changed. The default value is “public”.

Allowed characters in the **Community String** are as follows: **a-z**, **A-Z**, **0-9**, **_.-@()?#%^+~!**.

SNMP Contact

This option allows the SNMP Contact string to be changed. For example, this could be e-mail address of the administrator of the Multi-Tenant LoadMaster.

SNMP Location

This option allows the SNMP location string to be changed.

SNMP traps

When an important event happens to a Multi-Tenant LoadMaster, a Virtual Service or a Real Server, a trap is generated. These are sent to the SNMP trap sinks.

Enable/Disable SNMP Traps

This toggle option enables and disables the sending of SNMP traps.

> SNMP traps are disabled by default.

Send SNMP traps from the shared address

> This check box is only visible when the LoadMaster is in HA mode.

By default, SNMP traps are sent using the IP address of the master HA unit as the source IP address. Enabling this option will send SNMP traps from the master HA unit using the shared IP address.

SNMP Trap Sink1

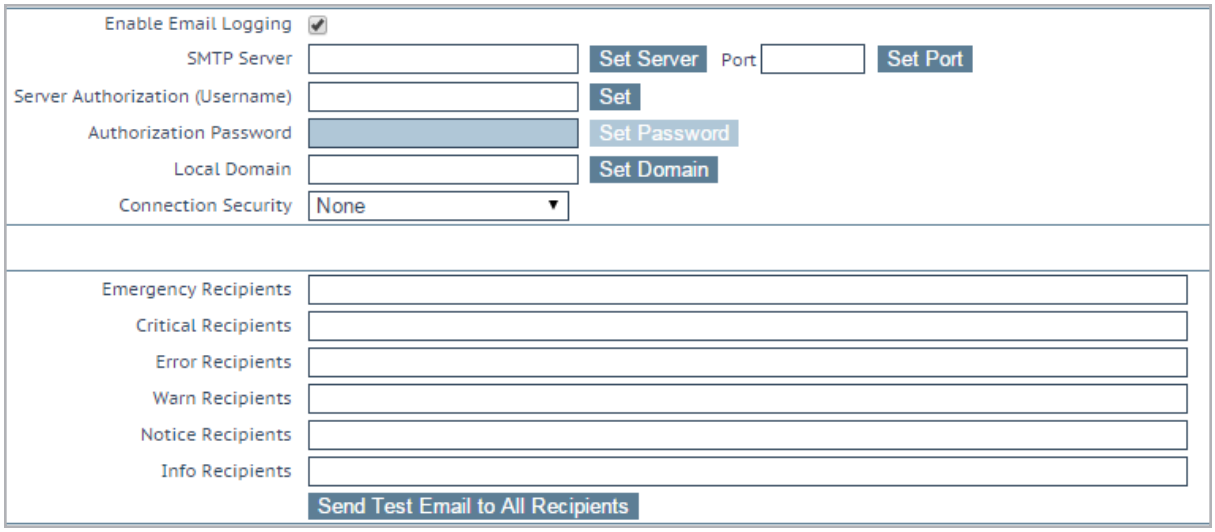
This option allows the user to specify a list of hosts to which a SNMPv1 trap will be sent when a trap is generated.

SNMP Trap Sink2

This option allows the user to specify a list of hosts to which a SNMPv2 trap will be sent when a trap is generated.

2.5.10.4 Email Options

This screen permits the configuration of email alerting for Multi-Tenant LoadMaster events. Email notification can be delivered for six predefined informational levels. Each level can have a distinct email address and each level supports multiple email recipients. Email alerting depends on a mail server, support for both an open relay mail server and a secure mail server is provided.



SMTP Server

Enter the FQDN or IP address of the mail server. If you are using FQDN please make sure to set the DNS Server.

Port

Specify the port of the SMTP server which will handle the email events.

Server Authorization (Username)

Enter the username if your mail server requires authorization for mail delivery. This is not required if you mail server does not require authorization.

Authorization Password

Enter the password if your mail server requires authorization for mail delivery. This is not a required if you mail server does not require authorization.

Local Domain

Enter the top-level domain, if your mail server is part of a domain. This is not a required parameter.

Connection Security

Select the type of security for the connection;

- None
- STARTTLS, if available
- STARTTLS

- SSL/TLS

Set Email Recipient

In the various **Recipients** text boxes, enter the email address that corresponds with the level of notification desired. Multiple email addresses are supported by a comma-separated list, such as:

Info Recipients: info@kemptechnologies.com, sales@kemptechnologies.com

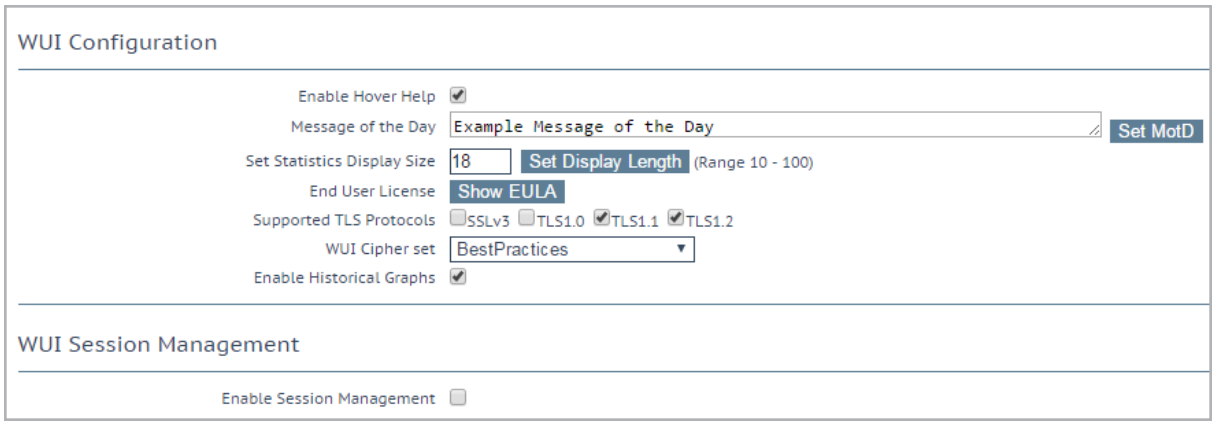
Error Recipients: support@kemptechnologies.com

Clicking the **Send Test Email to All Recipients** button sends a test email to all the listed email recipients.

2.5.11 Miscellaneous Options

2.5.11.1 WUI Settings

Only the **bal** user or users with 'All Permissions' set can use this functionality. Users with different permissions can view the screen but all buttons and input fields are grayed out.



Enable Hover Help

Enables blue hover notes shown when the pointer is held over certain fields.

Message of the Day (MOTD)

Type in text into the field and click the **Set MotD** button. This message will be displayed within the Multi-Tenant LoadMaster home screen.

> The maximum allowed message length is 5,000 characters. HTML is supported, but not required.

Set Statistics Display Size

This sets the maximum number of rows that can be displayed in the Statistics page. The allowable range is between 10 and 100 rows being displayed on the page.

End User License

Click the **Show EULA** button to display the Multi-Tenant LoadMaster End User License Agreement.

Supported TLS Protocols

Checkboxes are provided here which can be used to specify whether or not it is possible to connect to the Multi-Tenant LoadMaster WUI using the following protocols; SSLv3, TLS1.0, TLS1.1 or TLS1.2. TLS1.1 and TLS1.2 are enabled by default. It is not recommended to only have SSLv3 selected because SSLv3 is only supported by some old browsers. When connecting to the WUI using a web browser, the highest security protocol which is mutually supported by both the browser and the WUI will be used.

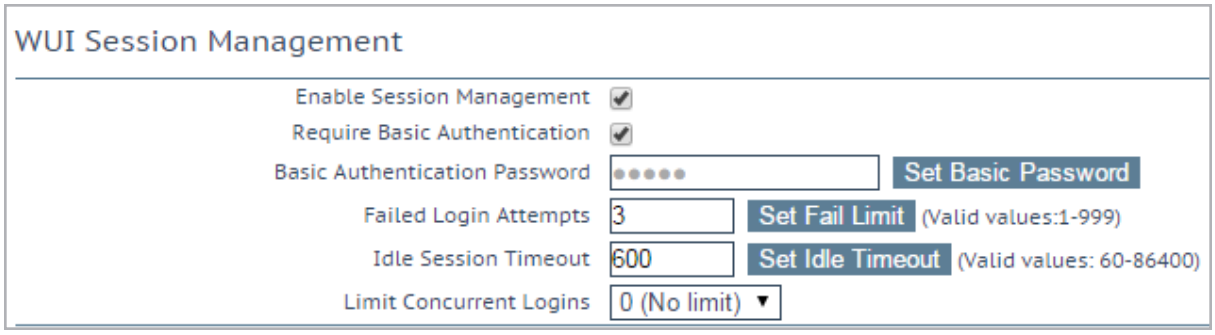
WUI Cipher set

Select the relevant cipher set to use for WUI access. For information on each of the cipher sets available, refer to the **Cipher Sets** section.

Enable Historical Graphs

Enable the gathering of historical statistics for the Virtual Services and Real Servers.

2.5.11.2 WUI Session Management



Session management is enabled by default on all Multi-Tenant LoadMasters initially deployed with firmware version MT_7.1.35 or above.

Only the **bal** user can enable or disable Session Management and/or Basic Authentication.

Users with the 'All Permissions' permission set can view the **Enable Session Management**, **Require Basic Authentication** and the **Basic Authentication Password** fields. However, users with the 'All Permissions' permission set can configure the **Failed Login Attempts** and **Idle Session Timeout** values.

Users with the 'User Administration' permissions set can view the screen but all buttons and input fields are grayed out.

All other users cannot view the **WUI Session Management**, **Currently Active Users** or **Currently Blocked Users** sections of the **WUI Configuration** screen.

When using WUI Session Management, it is possible to use one or two steps of authentication.

If the **Enable Session Management** check box is ticked and **Require Basic Authentication** is disabled, the user only needs to log in using their local username and password. Users are not prompted to log in using the **bal** or **user** logins.

If the **Enable Session Management** and **Require Basic Authentication** check boxes are both selected, there are two levels of authentication enforced in order to access the Multi-Tenant LoadMaster WUI. The initial level is Basic Authentication where users login using the **bal** or **user** logins, which are default usernames defined by the system.

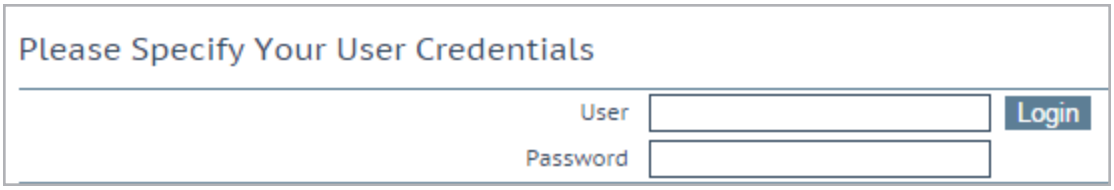
Once logged in using Basic Authentication, the user then must log in using their local username and password to begin the session.

Enable Session Management

Selecting the **Enable Session Management** check box enables the WUI Session Management functionality. This will force all users to initially log in to the server using either the **bal** or **user** logins and then to login to the session using their normal credentials.

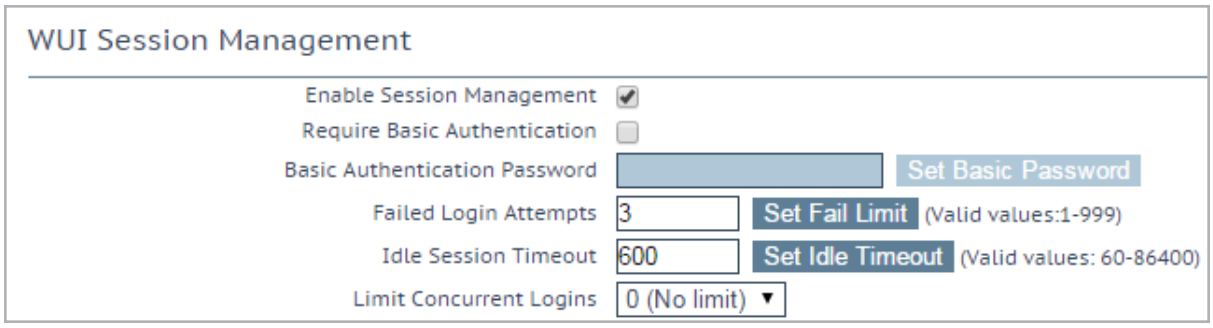
When this check box is selected, the user is required to log in to use Multi-Tenant LoadMaster.

> LDAP users need to login using the full domain name. For example an LDAP username should be **test@kemp.com** and not just **test**.



After a user has logged in, they may log out by clicking the button,  , in the top right-hand corner of the screen.

Once the WUI Session Management functionality is enabled, all the WUI Session Management options appear.



Require Basic Authentication

If WUI Session Management and Basic Authentication are both enabled, there are two levels of authentication enforced in order to access the Multi-Tenant LoadMaster WUI. The initial level is Basic Authentication where users login using the **bal** or **user** logins, which are default usernames defined by the system.

Once logged in using Basic Authentication, the user then must log in using their local username and password to begin the session.

Basic Authentication Password

The Basic Authentication password for the **user** login can be set by typing the password into the **Basic Authentication Password** text box and clicking the **Set Basic Password** button.

The password needs to be at least 8 characters long and should be a mix of alpha and numeric characters. If the password is considered to be too weak, a message appears asking you to enter a new password.

Failed Login Attempts

The number of times that a user can fail to login correctly before they are blocked can be specified within this text box. The valid values that may be entered are numbers between **1** and **999**.

If a user is blocked, only the **bal** user or other users with **All Permissions** set can unblock a blocked user.

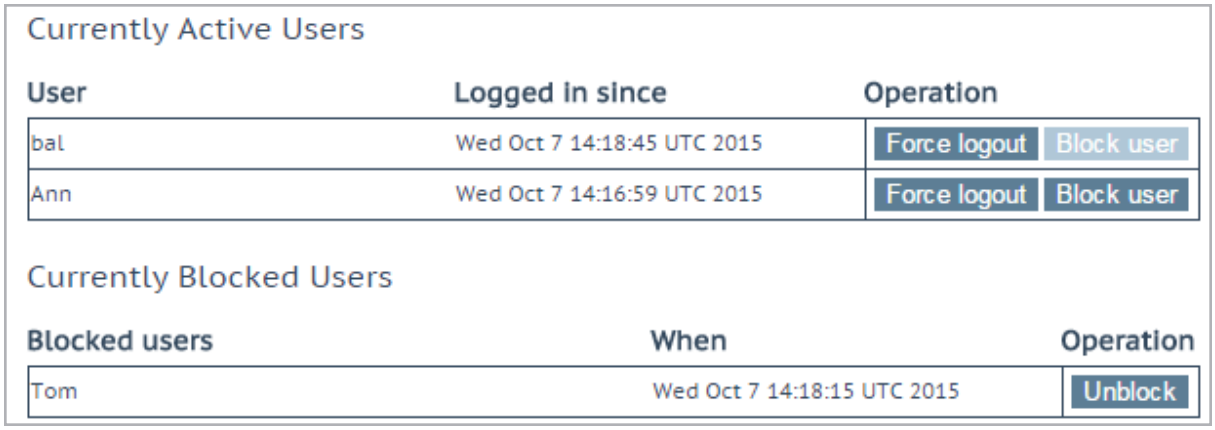
If the **bal** user is blocked, there is a 'cool-down' period of ten minutes before the **bal** user can login again.

Idle Session Timeout

The length of time (in seconds) a user can be idle (no activity recorded) before they are logged out of the session. The valid values that may be entered are numbers between **60** and **86400** (between one minute and 24 hours).

2.5.11.2.1 Active and Blocked Users

Only the **bal** user or users with 'All Permissions' set can use this functionality. Users with 'User Administration' permissions set can view the screen but all buttons and input fields are grayed out. All other users cannot view this portion of the screen.



Currently Active Users

The user name and login time of all users logged into the Multi-Tenant LoadMaster are listed in this section.

To immediately log out a user and force them to log back into the system, click the **Force logout** button.

To immediately log out a user and to block them from being able to log in to the system, click the **Block user** button**.** The user will not be able to log back in to the system until they are unblocked or until the Multi-Tenant LoadMaster reboots. Clicking the **Block user** button does not force the user to log off; to do this, click the **Force logout** button.

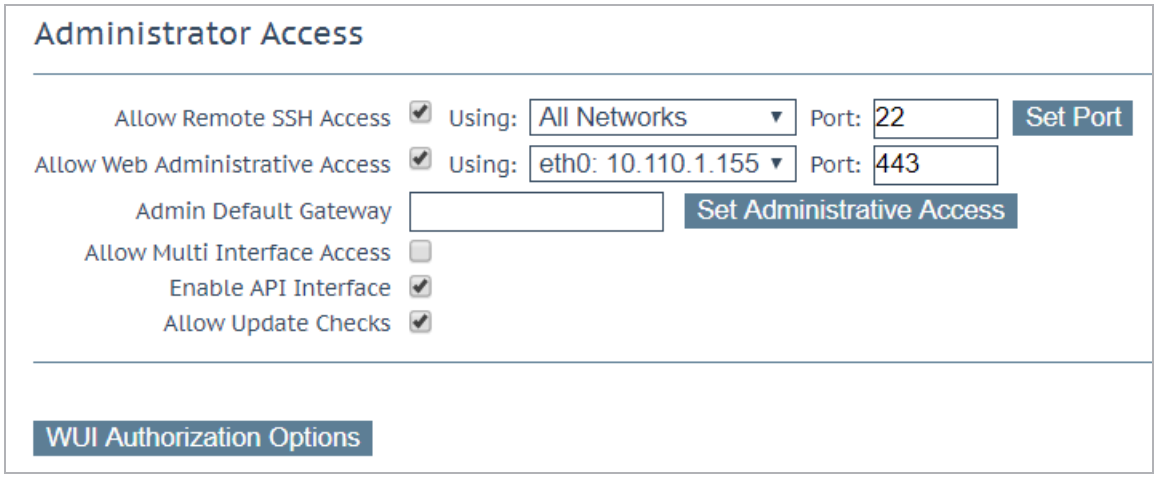
If a user exits the browser without logging off, that session will remain open in the currently active users list until the timeout has reached. If the same user logs in again, before the timeout is reached, it would be within a separate session.

Currently Blocked Users

The user name and login time of when the user was blocked are listed within this section.

To unblock a user to allow them to log in to the system, click the **Unblock** button.

2.5.11.3 Remote Access



Allow Remote SSH Access

You can limit the network from which clients can connect to the SSH administrative interface on Multi-Tenant LoadMaster.

Using

Specify which addresses that remote administrative SSH access to the Multi-Tenant LoadMaster is allowed.

Port

Specify the port used to access the Multi-Tenant LoadMaster using the SSH protocol.

Allow Web Administrative Access

Selecting this check box allows administrative web access to the Multi-Tenant LoadMaster. Disabling this option will stop access upon the next reboot.

> Disabling web access is not recommended.

Using

Specify the addresses that administrative web access is to be permitted.

Port

Specify the port used to access the administrative web interface.

Administrative Default Gateway

When administering the Multi-Tenant LoadMaster from a non-default interface, this option allows the user to specify a different default gateway for administrative traffic only.

> If the **Administrative Default Gateway** is being changed to another interface that is not accessible without proper routing, a static route into the Multi-Tenant LoadMaster should be added before changing the administrative interface IP. Once the routing is in please, the interface can be switched and the administrative default gateway can be selected if required. Then the static route can be removed.

Enable API Interface

Enables/disables the RESTful Application Program Interface (API).

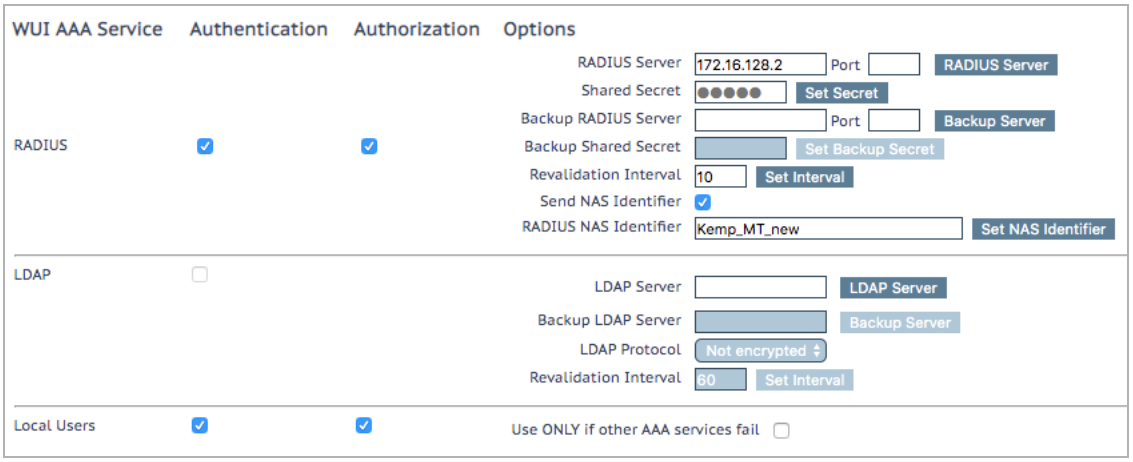
Allow Update Checks

Allow the Multi-Tenant LoadMaster to regularly check the Kemp website for new software versions.

2.5.11.4 WUI Authentication and Authorization

WUI Authorization Options

Click the **WUI Authorization Options** button on the **Remote Access** screen to display the **WUI Authentication and Authorization** screen. This option is only available when **Session Management** is enabled.



The **WUI Authentication and Authorization** screen enables the administration of the available authentication (login) and authorization (allowed permissions) options.

Authentication

Users must be authenticated before logging on to the Multi-Tenant LoadMaster. The Multi-Tenant LoadMaster allows authentication of users to be performed using the RADIUS and LDAP authentication methods as well as Local User authentication.

When all authentication methods are selected, the Multi-Tenant LoadMaster attempts to authenticate users using the authentication methods in the following order:

1. RADIUS
2. LDAP
3. Local Users

For example, if the RADIUS server is not available then the LDAP server is used. If the LDAP server is also not available, then Local User authentication methods are used.

If neither RADIUS nor LDAP authentication methods are selected, then the Local User authentication method is selected by default.

Authorization

The Multi-Tenant LoadMaster allows the users to be authorized by either RADIUS or using Local User authorization. The user's authorization decides what level of permissions the user has and what functions on the Multi-Tenant LoadMaster they are allowed to perform.

> The **RADIUS Authentication** check box must be enabled to use the **RADIUS Authorization** method. Authentication is for access (to ensure the user has a valid username and password) and authorization is used for permissions.

When both authorization methods are selected, the Multi-Tenant LoadMaster initially attempts to authorize the user using RADIUS. If this authorization method is not available, the Multi-Tenant LoadMaster attempts to authorize the user using the Local User authorization. Authorization using LDAP is not supported.

If neither RADIUS nor LDAP authentication methods are selected, then the Local User authentication method is selected by default.

You must configure the RADIUS server that you are using to authorize the same user permissions that appear on the WUI's user permissions page (with the exception of 'All Permissions'). The Reply-Message returned by the RADIUS server indicates the permissions it is allowing. On a Linux system, the message looks similar to the following:

LMUSER Cleartext-Password := "1fourall"Reply-Message = "real,vs,rules,backup,certs,cert3,certbackup,users"

The preceding example is of a RADIUS user configuration on a RADIUS server deployed on a Linux system. The LoadMaster determines the user's permissions from the "Reply-Message" (the permissions are similar to the ones for a local WUI user on the LoadMaster).

> The **bal** user is always authenticated and authorized using the Local User authentication and authorization methods. Disabling Local User authentication does not lock out the **bal** user. **Bal** is an admin/super user and is allowed to log in to the LoadMaster WUI even if Local User Authentication is disabled on the LoadMaster.

RADIUS Server Configuration

RADIUS Server

The IP address and Port of the RADIUS Server that is to be used to authenticate user WUI access to the Multi-Tenant LoadMaster.

Shared Secret

This input field is for the Shared Secret of the RADIUS Server.

A Shared Secret is a text string that serves as a password between the Multi-Tenant LoadMaster and the RADIUS server.

Backup RADIUS Server

The IP address and Port of the backup RADIUS Server that is to be used to authenticate user WUI access to the Multi-Tenant LoadMaster. This server will be used in case of failure of the main RADIUS Server.

Backup Shared Secret

This text box is to enter the Shared Secret of the backup RADUS Server.

Revalidation Interval

Specifies how often a user should be revalidated by the RADIUS server.

Send NAS Identifier

If this check box is disabled (default), a NAS identifier is not sent to the RADIUS server. If it is enabled, a Network Access Server (NAS) identifier string is sent to the RADIUS server. By default, this is the hostname. Alternatively, if a value is specified in the **RADIUS NAS Identifier** text box, this value is used as the NAS identifier. If the NAS identifier cannot be added, the RADIUS access request is still processed.

Sending the NAS identifier serves two purposes:

- It helps to classify the device type that is sending the request as opposed to simply sending the host IP address which makes troubleshooting and consuming logs easier.
- It enables customized authentication responses to be sent back from the server based on the identifier.

RADIUS NAS Identifier

If the **Send NAS Identifier** check box is selected, the **RADIUS NAS Identifier** field is shown. When specified, this value is used as the NAS identifier. Otherwise, the hostname is used as the NAS identifier. If the NAS identifier cannot be added, the RADIUS access request is still processed.

LDAP

LDAP Server

Specify the LDAP server to use. You can also specify a port number, if required.

Backup LDAP Server

The IP address and Port of the backup LDAP Server that is to be used to authenticate user WUI access to the Multi-Tenant LoadMaster. This server will be used in case of failure of the main LDAP Server.

LDAP Protocol

Select the transport protocol to use when communicating with the LDAP server.

> If you create an SSO domain with the **Authentication Protocol** set to **Certificates**, ensure to set the **LDAP Protocol** to **LDAPS**.

Revalidation Interval

Specify how often you should revalidate the user with the LDAP server.

Local Users

Use ONLY if other AAA services fail

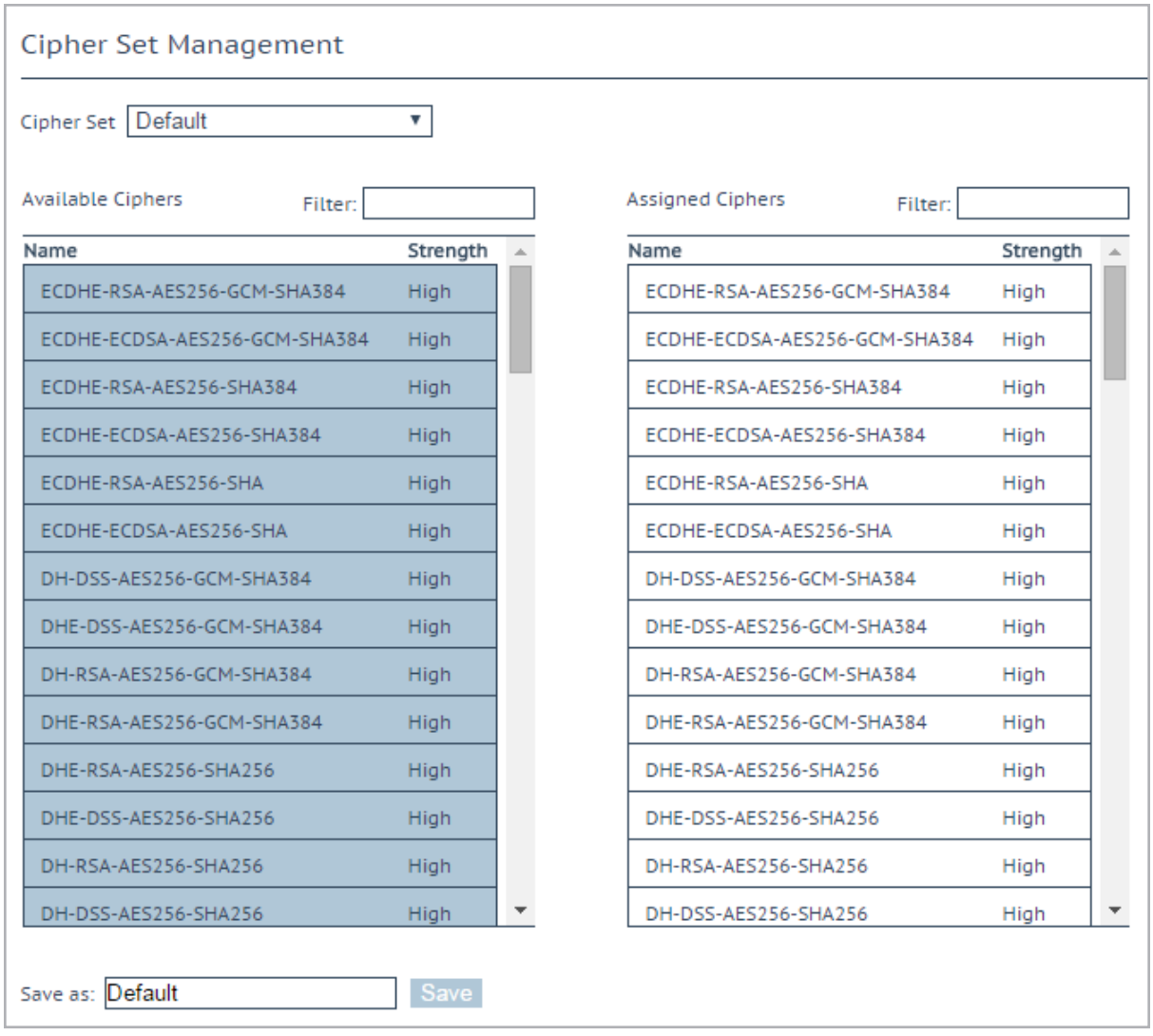
When selected, the Local Users authentication and authorization methods are used only if the RADIUS and/or LDAP authentication and authorization services fail to respond/time out.

Test AAA for User

To test a user's credentials, enter their username and password in the **Username** and **Password** fields and click the **Test User** button.

A message appears to inform you whether the user is validated or not. This is a useful utility to check a user's credentials without having to log in or out.

2.5.11.5 Cipher Sets



Cipher Set

Select the cipher set to view/modify.

The system-defined cipher sets are as follows:

- **Default:** The current default set of ciphers in the Multi-Tenant LoadMaster.
- **Default_NoRc4:** The Default_NoRc4 cipher set contains the same ciphers as the default cipher set, except without the RC4 ciphers (which are considered to be insecure).
- **BestPractices:** This is the recommended cipher set to use. This cipher set is for services that do not need backward compatibility - the ciphers provide a higher level of security. The configuration is compatible with Firefox 27, Chrome 22, IE 11, Opera 14 and Safari 7.
- **Intermediate_compatibility:** For services that do not need compatibility with legacy clients (mostly Windows XP), but still need to support a wide range of clients, this configuration is recommended. It is compatible with Firefox 1, Chrome 1, IE 7, Opera 5 and Safari 1.
- **Backward_compatibility:** This is the old cipher suite that works with clients back to Windows XP/IE6. This should be used as a last resort only.
- **WUI:** This is the cipher set recommended to be used as the WUI cipher set. The WUI cipher set can be selected in the **WUI Settings** screen. For further information, refer to the **WUI Settings** section.
- **FIPS:** Ciphers which conform to FIPS (Federal Information Processing Standards).
- **Legacy:** This is the set of ciphers that were available on the old Multi-Tenant LoadMaster firmware (v7.0-10) before OpenSSL was updated.

Refer to the **SSL Accelerated Services, Feature Description** for a full list of the ciphers supported by the Multi-Tenant LoadMaster, and a breakdown of what ciphers are in each of the system-defined cipher sets.

> Kemp can change the contents of these cipher sets as required based on the best available information.

Two lists are displayed – **Available Ciphers** and **Assigned Ciphers**. These lists can be filtered by typing some text into the **Filter** text boxes provided. iThe **Filter** text boxes will only allow you to enter valid text which is contained in the cipher names, for example **ECDHE**. If invalid text is entered, the text box will turn red and the invalid text is deleted.

Ciphers can be dragged and dropped to/from the **Available** and **Assigned** lists as needed. Ciphers which are already assigned will appear greyed out in the **Available Ciphers** list.

Changes cannot be made to a preconfigured cipher set. However, you can start with a preconfigured cipher set – make any changes as needed and then save the cipher set with a new custom name. Enter the new name in the **Save as** text box and click the **Save** button. Custom cipher sets can be used across different Virtual Services and can be assigned as the WUI cipher set.

It is not possible to delete preconfigured cipher sets. However, custom cipher sets can be deleted by selecting the relevant custom cipher set and clicking the **Delete Cipher set** button.

2.5.11.6 Network Options

Enable Alternate GW support

If there is more than one interface enabled, this option provides the ability to move the default gateway to a different interface.

Enabling this option adds another option to the **Interfaces** screen – **Use for Default Gateway**.

Enable Strict IP Routing

When this option is selected, only packets which arrive at the machine over the same interface as the outbound interface are accepted.

Enable DHCP for MT VNF(s)

This check box specifies whether or not the MT guests should utilise DHCP for initial IP configuration. If this is enabled, the initial IP address and default gateway of the guest VNF will be automatically obtained using DHCP, and you will not be prompted to set them. If this option is disabled, text boxes will be displayed when creating an instance which allow you to specify the initial IP address and default gateway.

This check box is also displayed after the initial Multi-Tenant LoadMaster installation when you are prompted to instantiate an initial VLM VNF, but the option is called **Use DHCP for guest VNF(s)**.

SDN Controller

Specify the address of an SDN controller to connect to.

HTTP(S) Proxy

Specify the HTTP(S) proxy server and port the Multi-Tenant LoadMaster will use to access the internet.

References

Unless otherwise specified, the following documents can be found at http://kemptechnologies.com/documentation.

Licensing, Feature Description

Virtual Services and Templates, Feature Description

Multi-Tenancy, Feature Description

Kemp Multi-Tenant LoadMaster, Product Overview

Radius Authentication and Authorization, Technical Note

SSL Accelerated Services, Feature Description

Last Updated Date

This document was last updated on 17 October 2019.