Progress®
Kemp® LoadMaster®

Feature Description High Availability (HA)

Generated on: 18 December 2024

Copyright

Visit the following page online to see Progress Software Corporation's current Product Documentation Copyright Notice/Trademark Legend: Product Documentation Copyright Notice & Trademarks | Progress

Table of Contents

Chapter 1: Introduction 5

Chapter 2: Advantages of High Availability (HA) 7

Chapter 3: Prerequisites 8

Chapter 4: HA Issues on VMware 10

Chapter 5: HA Components. 12

Chapter 6: Set Up HA 14

Set the Partner Shared Secret 14

Set up the First Unit. 15

Set up the Second Unit 19

Enable the 'Use for HA Checks' Option. 22

Test Failover 23

Chapter 7: Performing a Firmware Update on HA Pairs 25

Chapter 8: HA WUI Options 26
Partner Communications 26
HA and Clustering 28
Interfaces 28
HA Parameters 29

Chapter 9: Troubleshooting. 39
General Troubleshooting Tips 40
Confirm Settings 40
Further Details about IGMP Snooping and PortFast 42
No HA Status Squares are Visible in the WUI. 43
Green/Red HA Status Squares 43
Blue HA Status Square 44
Both Units are Active and the WUI is Unresponsive - Blue or Red Status Square 44
Gray HA Status Square. 45
Virtual Services Temporarily Unavailable After Failover 45
No Access to WUI on HA1/2 or Shared 45
Nothing Works. 46
Issue with Hyper-V and HA on a Pair of VLMs 46
Synchronization Issue After Unbonding/Bonding an Interface 46
Log Messages Explanations 46

Chapter 10: Replacing Hardware HA Units 48

Chapter 11: Replacing Virtual HA Units 56

Chapter 12: References 65

1

Introduction

The High Availability (HA) feature of the LoadMaster guarantees the availability of your server farm. HA is achieved by a hot-standby, failover mechanism. Two identical LoadMaster units are integrated into the network as a HA pair. One machine serves as the active LoadMaster and the second one remains in a standby, idle state - always prepared to take over the activities from the active server. This pair appears as a single logical unit to the internet side and to the server farm side connections.

With a HA pair, each network interface has an individual IP address and one shared IP address which is shared with the partner unit. The shared IP address is identical for both LoadMaster appliances, though it is associated with only the active LoadMaster at any given time.

Note: A shared IP address must be added to all production interfaces.

Note: HA in the LoadMaster for cloud products works differently to that of a regular LoadMaster. For more information and instructions on how to configure HA on the LoadMaster for cloud products, refer to the relevant document on the Documentation Page.

You must have three IP addresses available for HA configuration purposes. These are required for the:

- Active unit
- Standby unit
- Shared interface

	Unit 1	Unit 2
Interface address	192.168.15.110	192.168.15.111

	Unit 1	Unit 2
Partner address	192.168.15.111	192.168.15.110
Shared IP address	192.168.15.112	192.168.15.112

For a one-armed configuration, only one interface is configured. Two individual Virtual IP (VIP) addresses are set on each LoadMaster unit as their physical IP address; one address for HA-1 and the other for HA-2. The third IP address is set for the shared IP address which is for the Web User Interface (WUI) management page and routing. Additional addresses are needed if there is a need to set up the HA pair as a two-arm configuration and configure more interfaces. Each additional interface configured requires three free IP addresses per interface.

Document Purpose

This document describes the HA feature in the LoadMaster and provides step-by-step instructions on how to configure HA (active/standby).

Note: If you want to have multiple units in an active/active configuration, review the LoadMaster Clustering Feature Description.

2

Advantages of High Availability (HA)

The goal of redundant LoadMasters is to provide reliable traffic management, even if one LoadMaster becomes unavailable. The advantages of HA are as follows:

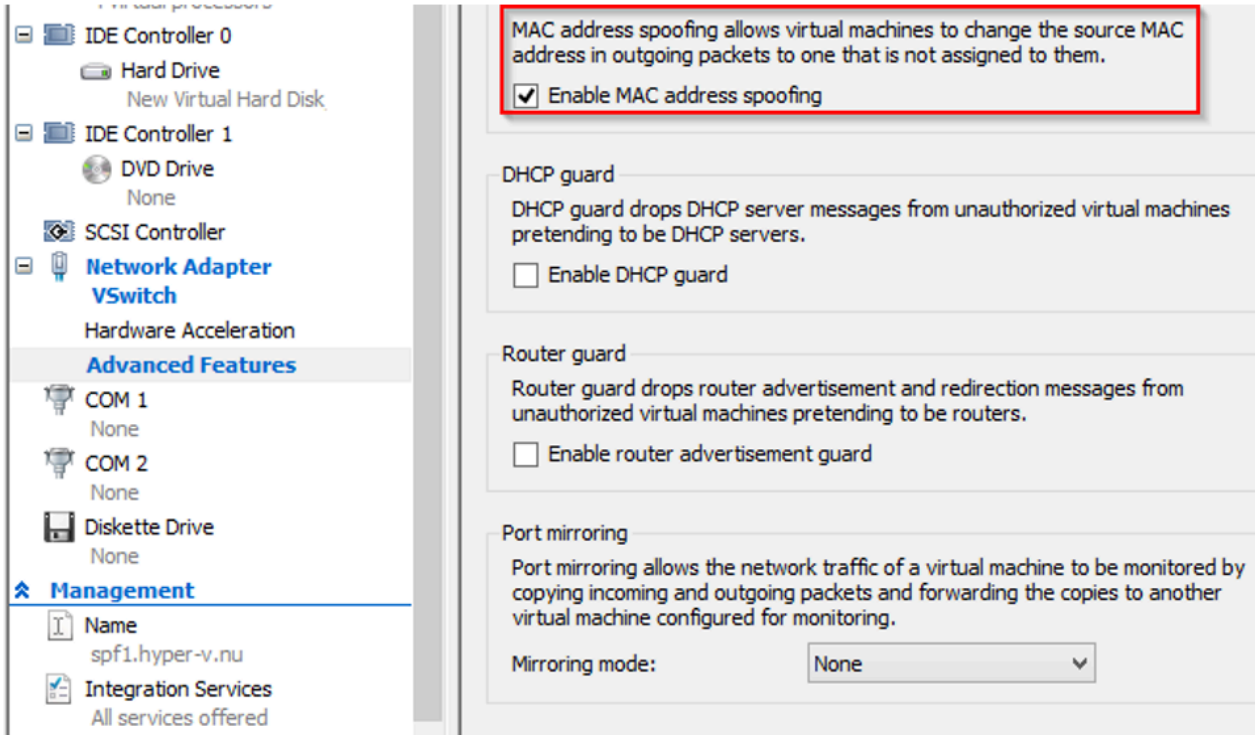
- Eliminates a single point of failure.
- The second (standby) unit monitors the active unit to detect if a failure has occurred.
- Persistence can be kept using the HA parameters:
  - Inter HA L4 TCP Connection Updates
  - Inter HA L7 Persistency Updates

3

Prerequisites

There are some prerequisites to be aware of before setting up HA:

- You must have two LoadMasters, each with its own license.
- If using physical LoadMasters, it is required that the two LoadMasters are:
  - Deployed.
  - Located on the same subnet.
  - In the same physical location.
  - Not located further than 100 meters from each other.
  - Using the same default gateway.
- A layer 2 connection (Ethernet/VLAN) is required.
- Multiprotocol Label Switching (MPLS) networks are not supported in a HA setup.
- Ensure that you have more than one interconnection between the two LoadMasters to avoid data loss or lack of availability.
- Use Network Time Protocol (NTP) to keep times on the LoadMasters up-to-date. This ensures that the times are correct on any logs and that Common Address Redundancy Protocol (CARP) message timestamps are in sync.



- Ensure that any switches do not prevent MAC spoofing. For example, on Hyper-V, go to the network adapter settings in the Virtual Machine settings and select the **Enable MAC address spoofing** check box.
- Latency on the link between the two LoadMasters must be below 100 milliseconds.
- By default, multicast traffic flow is required in both directions between the devices. This includes disabling Internet Group Management Protocol (IGMP) snooping on the various switches between the LoadMasters. Alternatively, you can instead enable HA communication between the HA LoadMasters using broadcast traffic. Refer to the HA Components section for further details.
- Three IP addresses are required for each subnet in which the LoadMaster is configured.
- The same LoadMaster models running the same release of LMOS must be used when configuring High Availability (HA) pairs.

4

HA Issues on VMware

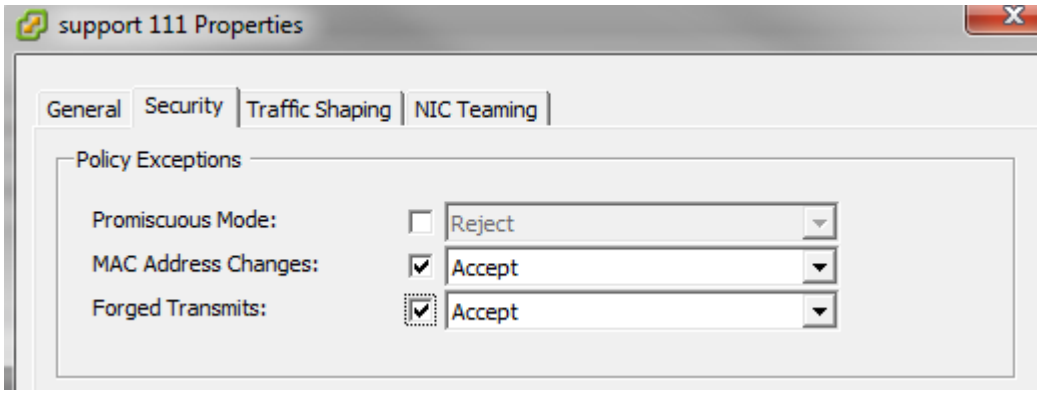
Refer to the sections below for some details about HA issues that may occur in a VMware environment.

Both Units Attempt to be the Active Unit





In some situations, when using HA in a VMware environment, both units might attempt to be the active unit and it may show the other unit as pacified (represented by a blue HA status square). This issue could be caused by the VMware Switch configuration. To resolve this issue, select the options as outlined below on the virtual switch.



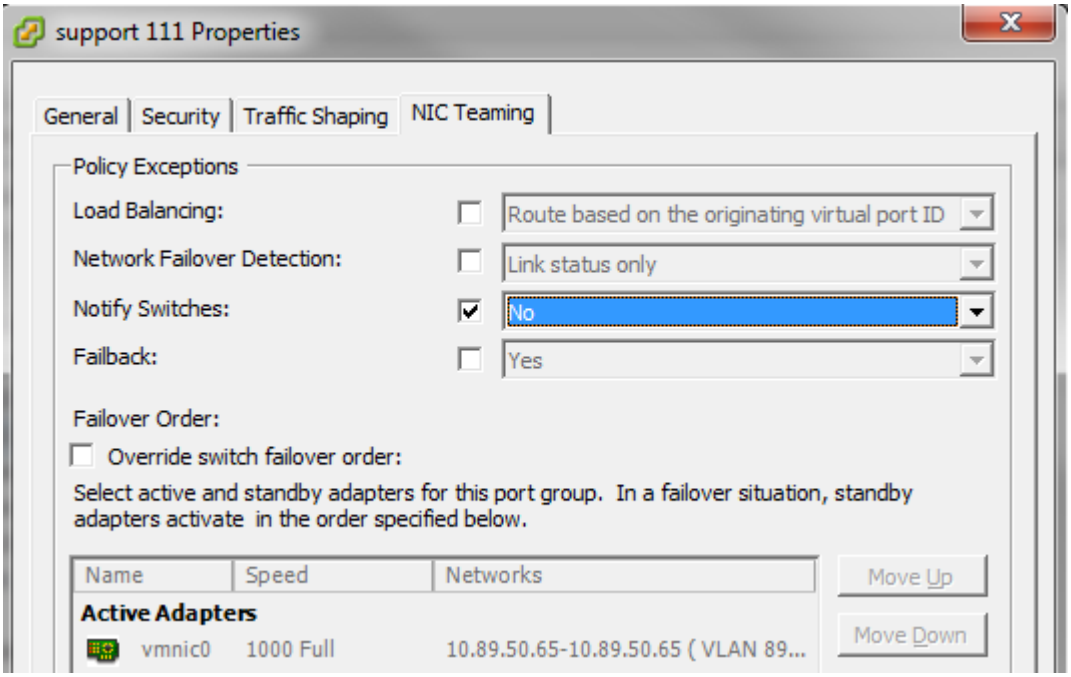
Ensure that **MAC Address Changes** and **Forged Transmits** are both selected. When they have been selected, reboot one of the LoadMasters.



The units should now be able to communicate properly. The correct state should now appear in the HA status icons.

Two Virtual LoadMasters on Different Hosts

Having two Virtual LoadMasters on different hosts can also pose problems on VMware.



To resolve these issues, select the **Notify Switches** check box in the **NIC Teaming** tab of the virtual switch and select **No** in the drop-down list.

5

HA Components

LoadMasters in a HA configuration use two protocols, CARP and Sync, to perform health checks and to synchronize the configuration between LoadMasters.

CARP:

- CARP is the HA protocol that the LoadMaster uses.
- Each HA unit provides health status updates to the other partner.
- The health status updates are used by the standby LoadMaster to decide when it is appropriate to assume the active role.
- On each interface, the **Use for HA Checks** option enables CARP requests to be sent over that interface. It can be **enabled on** multiple interfaces.
- By default, the LoadMaster uses multicast IP addresses (224.0.0.18) when sending CARP packets. Alternatively, when the **Use Broadcast IP address** option is enabled in the **HA Parameters** screen, the LoadMaster uses the broadcast address (255.255.255.255) to send CARP packets.
- CARP works in a similar way to Cisco's Virtual Router Redundancy Protocol (VRRP). For CARP to work between a pair of LoadMasters, both LoadMasters must be on the same broadcast domain.

Note: When CARP is used, packet analysis tools (such as Wireshark), incorrectly display the protocol used as Virtual Router Redundancy Protocol (VRRP). Any IP addresses displayed by the packet analysis tools are fictitious and are not part of the CARP protocol.

Sync:

- Sync maintains a 'single image view' of the LoadMaster settings. It keeps the LoadMaster up-to-date with

changes made to Virtual Services and all other configurations.

- Notable exceptions that are not synchronized are time and the password for the **bal** user.
- Keeps the standby LoadMaster updated on persistence updates.

6

Set Up HA

Refer to the following sections for details on how to set up HA LoadMasters.

Related Links

For details, see the following topics:

- Set the Partner Shared Secret
- Set up the First Unit
- Set up the Second Unit
- Enable the 'Use for HA Checks' Option
- Test Failover

Set the Partner Shared Secret

High Availability (HA) cannot be configured until the **Partner Shared Secret** is set.

The **Partner Shared Secret** is required to secure communications between partner devices and must be enabled on all HA partners, all LoadMasters in a cluster, and all GEO partners. The **Partner Shared Secret** must be the same on:

- Both units in a HA setup
- All units in a LoadMaster cluster

- All GEO partners
- All remote GEO machines that retrieve Virtual Services from this device

When an incoming shared secret does not match the local **IPartner Shared Secret** (including if only one side is providing a shared secret), a warn-level log message is recorded that says **Unauthorized Remote Machine connection from <ClientIPAddress>** and the connection fails.

You can find this secret in the following locations:

- Regular/shared Web User Interface (WUI): **Certificates & Security > Remote Access**
- Local WUI (of a configured HA or cluster unit): **Local Administration > Remote Access**

This secret must have a minimum of 8 and a maximum of 127 characters. The following characters are supported:

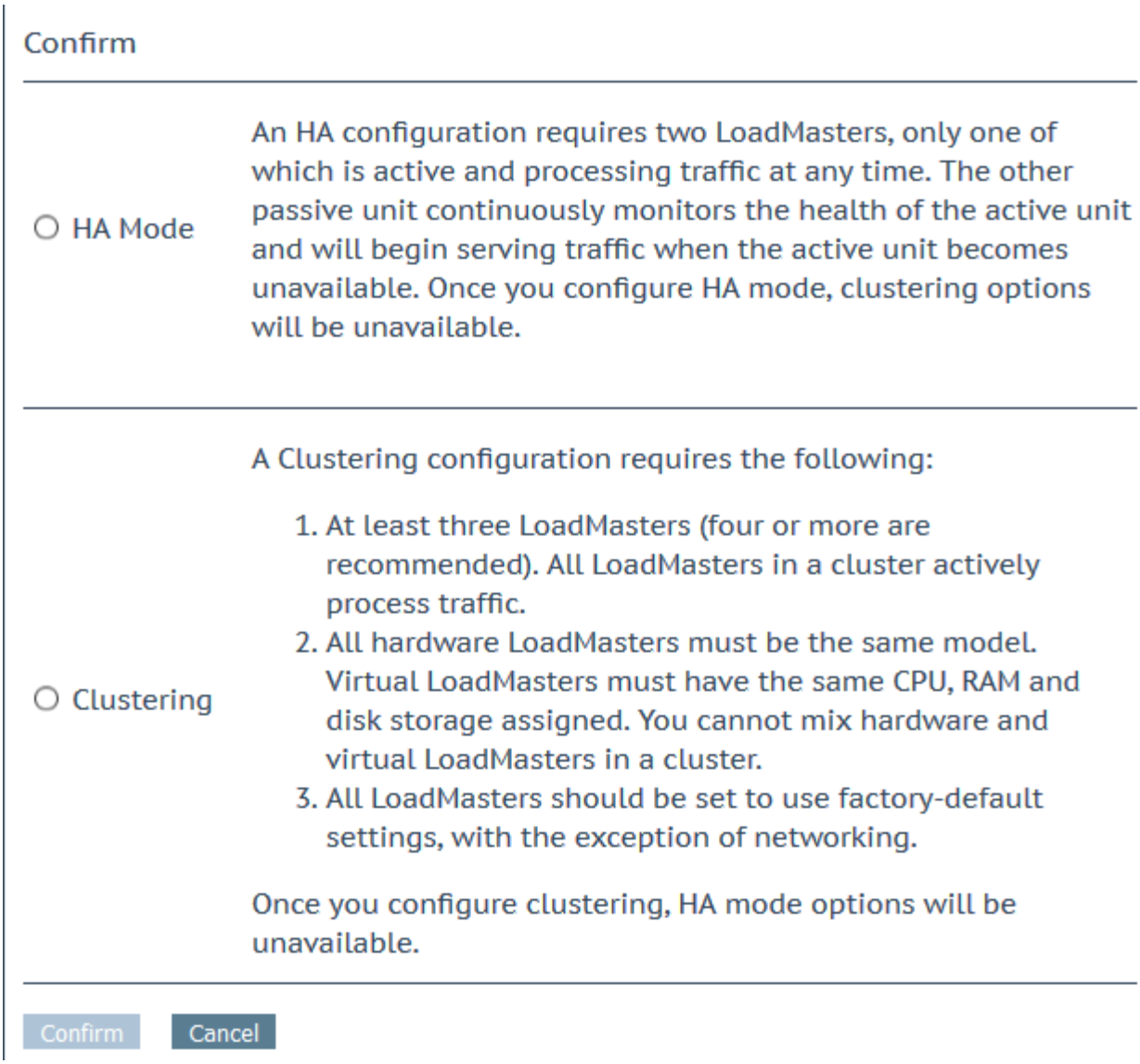
- Numeric: 0-9
- Uppercase alphabetic: A-Z
- Lowercase alphabetic: a-z
- Special characters: !"#$%&()*+,-./:;<=>?[\~]^_@`{|}

If you try to set up HA and the **Partner Shared Secret** has not been set, a pop-up message appears saying you need to set the secret. When you click **OK**, you are brought to the **Remote Access** screen to set the secret.

Set up the First Unit

To build a HA LoadMaster environment there are several settings that you must carefully specify. Follow the steps below to set up HA:

1. Log in to the LoadMaster that you want to be the active (master) unit.
2. In the main menu, select **System Configuration** and click **HA and Clustering**.

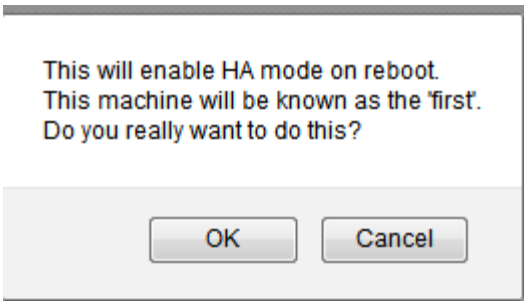


3. A screen appears asking if you want to set up **HA Mode** or **Clustering**. To set up HA, select **HA Mode** and click **Confirm**.

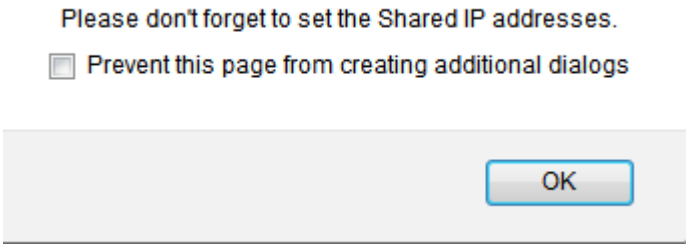


Note: For instructions on configuring clustering, refer to the **LoadMaster Clustering Feature Description** on the Documentation page.

4. Select **HA (First) Mode** in the **HA Mode** drop-down.

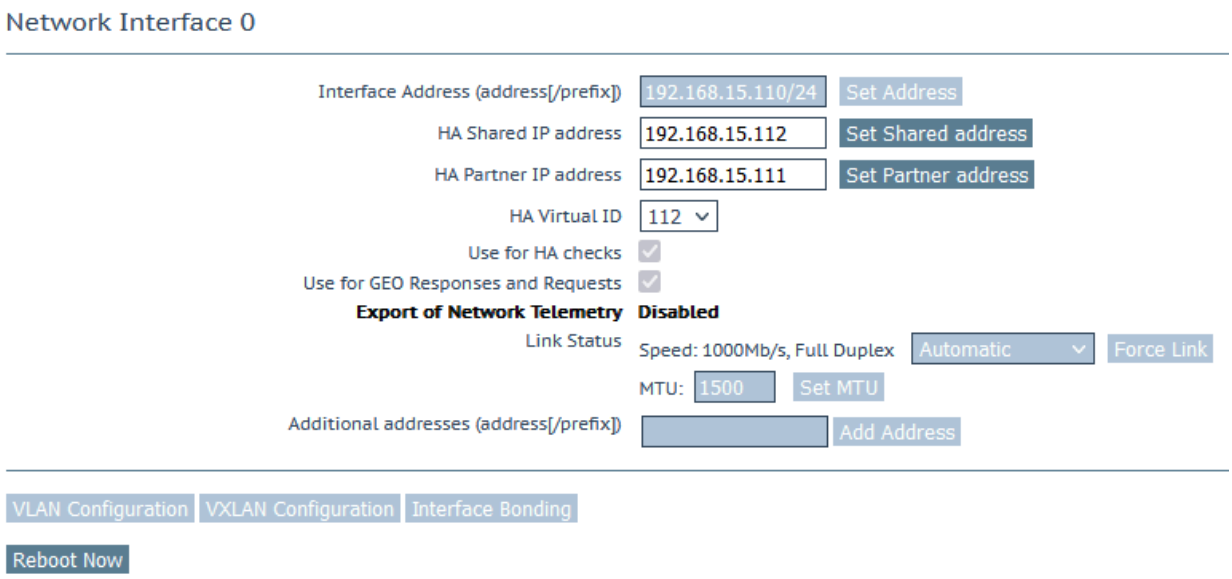


5. Click **OK**.



Note: Do not reboot at this time.

6. Click **OK** on the resulting message reminding not to forget to set the shared IP address.



Note: Selecting the **Prevent this page from creating additional dialogs** check box stops any warning messages, such as this one, from appearing.

7. Specify the desired shared IP address in the **HA Shared IP address** field and click **Set Shared address**.

Note: A shared IP address must be added to all production interfaces.

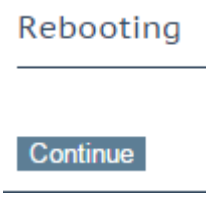
8. A confirmation message may appear. Click **OK**.

Note: Do not reboot or reconnect at this time.

9. Enter the IP address of the standby unit in the **HA Partner IP address** field and click **Set Partner address**.
10. A confirmation message appears. Click **OK**.
11. As of the 7.2.36 firmware, the LoadMaster selects a **HA Virtual ID** based on the shared IP address of the first configured interface (the last eight bits). You can change the value to whatever you want (in the range 10 – 255) or you can keep it at its existing value.

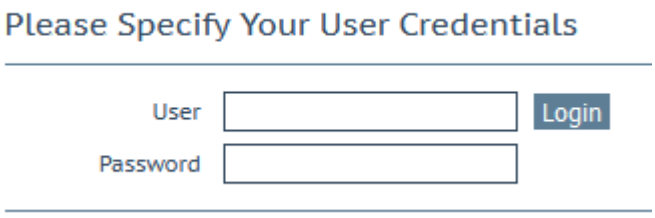
Note: Ensure the Virtual ID is unique for each HA pair on the network. When using multiple HA LoadMaster pairs (or other devices using CARP-like protocols) on the same network, this value uniquely identifies each HA pair so that there are no potential unwanted interactions.

12. Configure any other settings as needed.
13. Click **Reboot Now**.



14. Click **Continue**.
15. Refresh the page after the LoadMaster has rebooted (this may take a few minutes).

Note: A log in screen appears. After logging in, a different menu appears than before. This is the **Local Administration** menu displayed for HA units - this menu has fewer options. Only configuration settings pertaining to that specific unit are accessible using the **Local Administration** option. All management of the HA units should be done using the shared IP address. To see the full menu and configure the units, access the WUI of the shared IP address, which you configured previously.



16. Log in to the shared IP Web User Interface (WUI) by entering the shared IP address in the address bar of the browser and pressing **Enter**.

Note: In the top-right of the screen there are two indicator squares.  These squares indicate the status of the HA pair. The left square always represents HA1 and the right represents HA2. The **A** represents which unit is active. The first or second HA unit can be opened by clicking the relevant status icon. Green and green status colors indicate a properly paired configuration. Currently, the icons are green and red because the HA2 unit has not yet joined the pair. For an explanation of all icon colors and

statuses, refer to the HA Parameters section.

17. Go to **HA Parameters** in the main menu.
18. Enter a different number (different from the IDs of other HA devices) in the **HA Virtual ID** text box and click **Set Virtual ID**. Using the same ID as other HA devices may cause problems.

Note: All HA pairs on the network must be assigned unique **HA Virtual ID** numbers.

Note: Ensure the **Partner Shared Secret** matches in both the active and standby unit. You can find this secret in the following locations:

- Regular/shared WUI: **Certificates & Security > Remote Access**
- Local WUI (of a configured HA unit): **Local Administration > Remote Access**

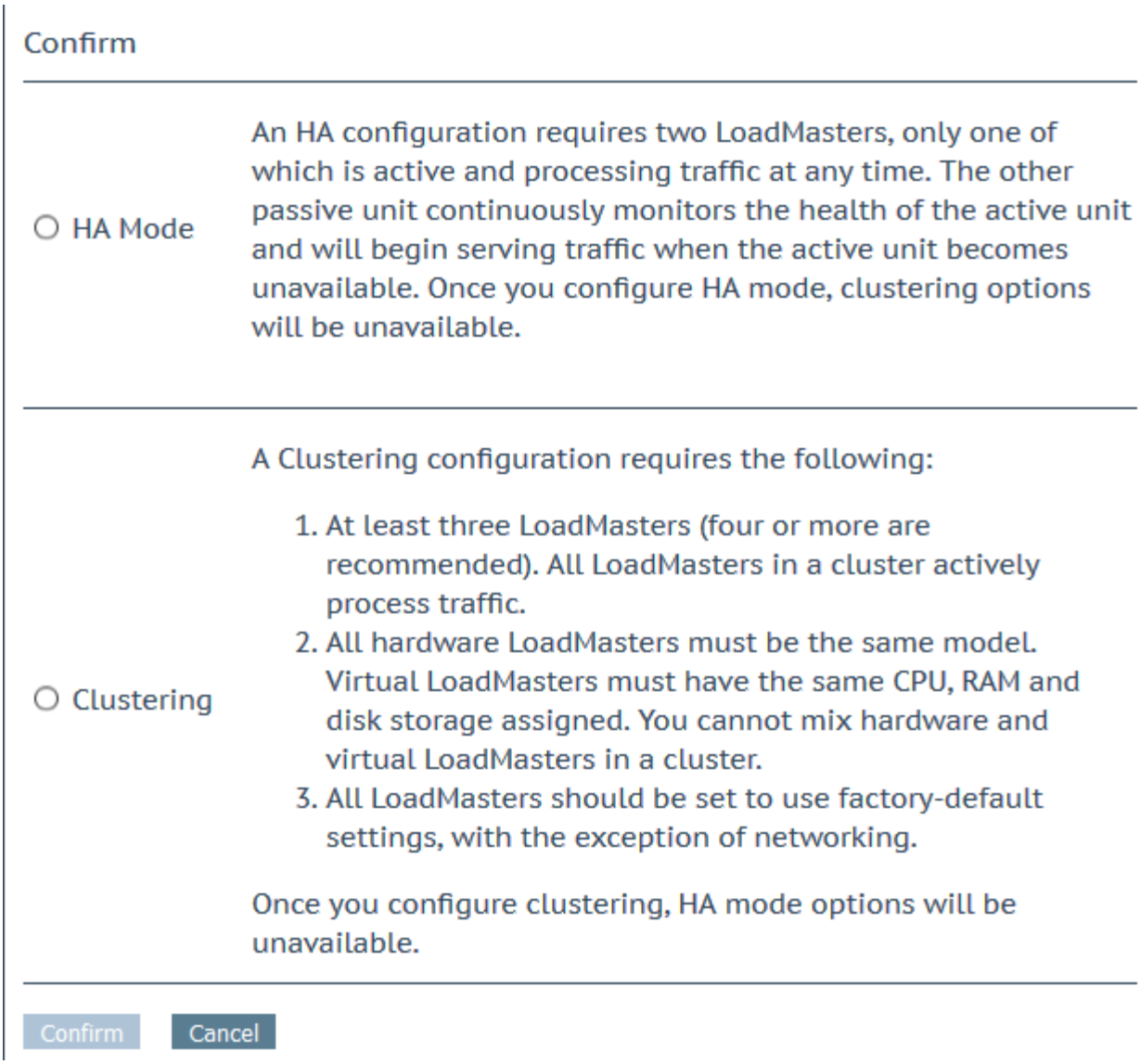
Set up the Second Unit

Now that HA has been configured on the first unit, the second unit must be set up. Follow the steps below to do this:

1. Enter the IP address of the second unit in the address bar of the browser and press **Enter**.

   Note: Ensure to enter **https://** before the IP address.

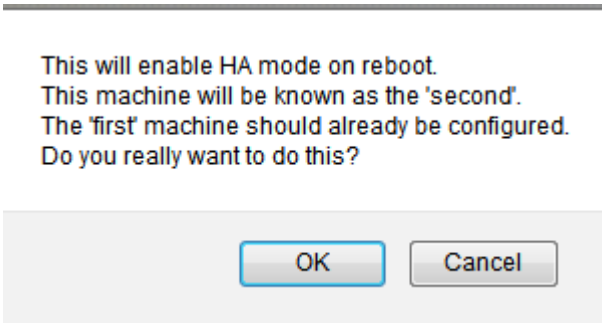
2. In the main menu, select **System Configuration** and click the **HA option**.



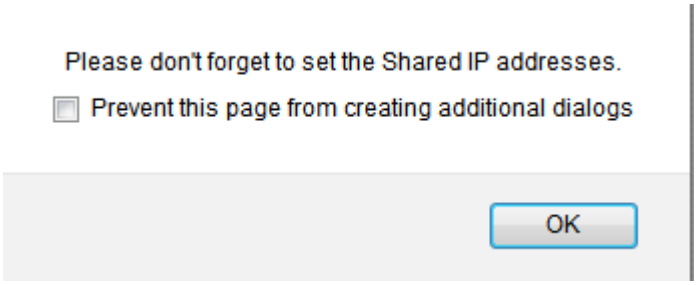
3. A screen appears asking if you want to set up **HA Mode** or **Clustering**. To set up HA, select **HA Mode** and click **Confirm**.



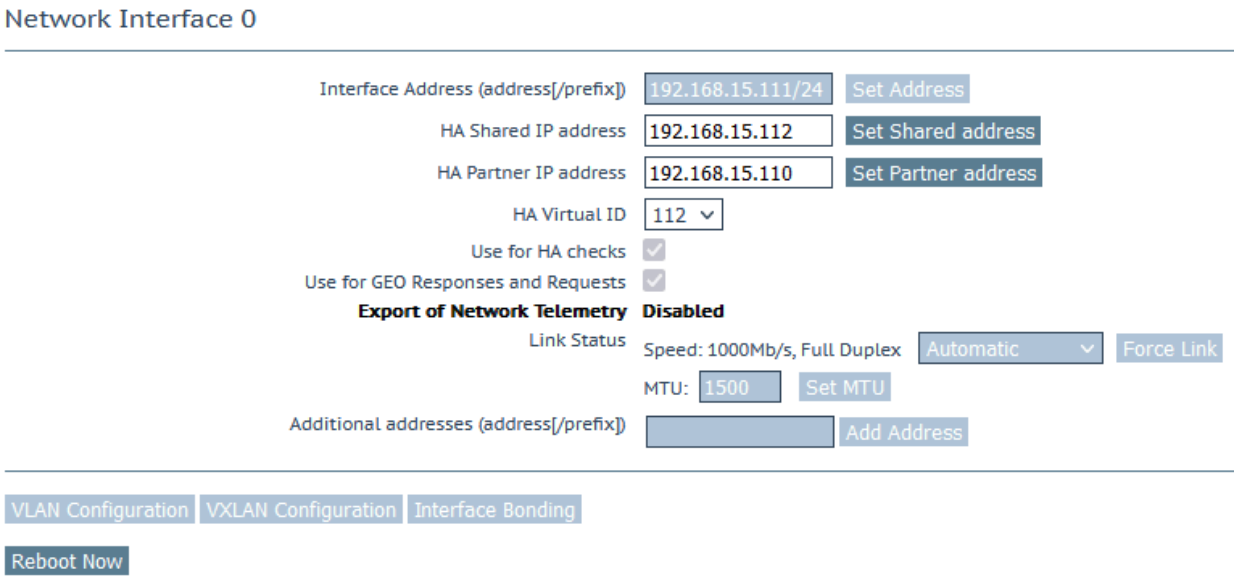
4. Select **HA (Second) Mode** as the **HA Mode**.



5. Click **OK**.



6. Click **OK**.



Note: To prevent any warning messages such as this one from appearing, select the **Prevent this page from creating additional dialogs** check box.

7. Enter the **HA Shared IP address** and click **Set Shared address**.

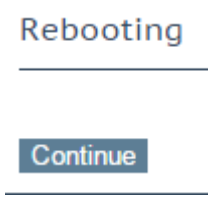
Note: A shared IP address must be added to all production interfaces.

Note: The **HA Shared IP address** must be the same as the **HA Shared IP address**, which was set when configuring the first unit in **the** Set up the First Unit section.

8. Click **OK**.
9. Click **OK** on the message asking to reconnect to the shared IP address.
10. Enter the IP address of the first (master) unit in the HA pair in the **HA Partner IP address** field and click **Set Partner address**.
11. Click **OK**.
12. Ensure the **HA Virtual ID** is the same as it is on the other unit.

Note: If they are not the same, the pairing fails.

13. Change any other settings as needed.
14. Click **Reboot Now**.



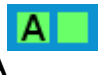
15. Click **Continue**.

Note: Passwords for the **bal** account are not synchronized across HA pairs, so ensure to use the same password on both units. Problems may occur if different passwords are used.

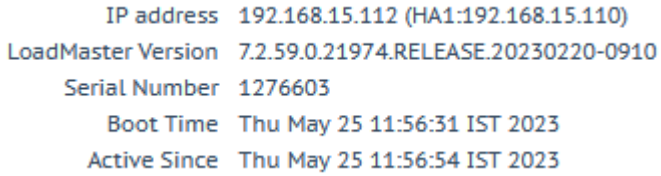
Note: Ensure the **Partner Shared Secret** matches in both the active and standby unit. You can find this secret in the following locations:

- Regular/shared WUI: **Certificates & Security > Remote Access**
- Local WUI (of a configured HA unit): **Local Administration > Remote Access**

After rebooting, the HA pair establishes a TCP connection (using port 6973) between the two addresses. The synchronization process is started for the configuration.

The indicator squares should now be green and green. 

The **A** indicates the active unit of the pair. If the first synchronization attempt fails (that is, the icons are not green and green) a second attempt might be needed.



On the home screen, the IP address field has changed. In addition to specifying the shared IP address of the pair, it also specifies the IP address of the unit. The left IP address is the shared address. The IP address in parentheses is the address of the current unit.

Enable the 'Use for HA Checks' Option

Some guidelines relating to the **Use for HA checks** option are below:

- The standby unit will not become active unless it does not receive a health check message from the active unit. So, all interfaces with **Use for HA checks** must fail or be blocked.
- The active unit will give up the role and become standby if any of its interfaces with **Use for HA checks**

enabled fails.

- In the past it was common practice to have a directly connected network cable between the two LoadMasters but this is no longer a supported configuration. This type of configuration causes the LoadMaster to think it is a production link and if one of the LoadMasters reboots, the other one fails too. This is why this type of setup is not supported.
- If the **Use for HA checks** check box is grayed out it means that this is the only interface configured to be used for HA checks and it cannot be deselected.

To enable the **Use for HA checks** option, follow the steps below:

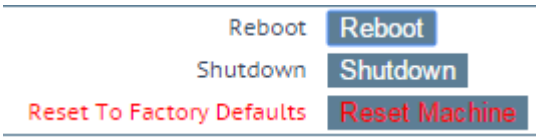
1. Go to the WUI of the shared IP address.
2. In the main menu, select **System Configuration**.
3. Select the relevant interface.
4. Select the **Use for HA checks** check box.

These steps can be repeated if you need to enable the **Use for HA checks** option on more than one interface.

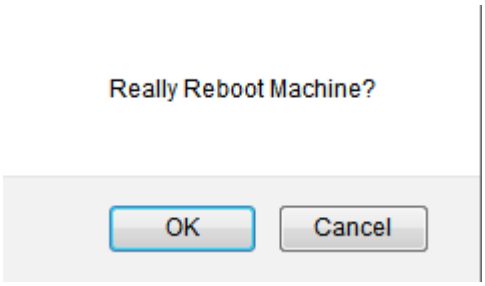
Test Failover

Now that the HA units have been set up, failover can be tested if needed. The easiest way to do this is to reboot the active unit. To reboot the unit, follow the steps below:

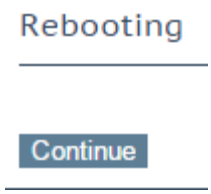
1. Log in to the IP address of the active unit.
2. In the main menu, click **Local Administration**.
3. Select **System Reboot**.



4. Click **Reboot**.



5. A confirmation message may appear. Click **OK**.



6. Click **Continue**.

When HA1 is back online, both HA status icons should be green. The **A** should have moved into the right green square.  This means that the secondary unit is now the active unit.

Note: When using local certificates in HA mode – the shared IP inherits the local certificate from the active unit. So, if a standby unit has a different local certificate to the active and failover occurs, the shared IP inherits the local certificate of the standby (now active) unit.

7

Performing a Firmware Update on HA Pairs

We recommend performing firmware updates outside of working hours. This ensures there is no interruption to client connectivity. If it has to be done during working hours, we recommend scheduling a maintenance window.

Note: Before updating the firmware, ensure the **Switch to Preferred Server** drop-down list is set to **No Preferred Host** in **System Configuration > HA Parameters**.

We recommend updating the passive unit first and then updating the active unit. This causes only a single failover and minimal downtime, and is the preferred option for most customers. While this procedure does leave the currently passive LoadMaster as the active LoadMaster going forward, this usually has no consequences in most customer environments. However, it is also possible to update the currently active unit, failover to the passive unit, update the passive unit and then failover to the originally active unit.

To update the firmware on a HA pair using the recommended method; perform the following steps using the shared IP address:

1. Update the passive LoadMaster first (we will refer to this LoadMaster as **B**).
2. When the update is complete, reboot **B**.
3. When unit **B** is back up, update the active unit (we will refer to this unit as **A**).
4. When the update is complete, reboot **A**. Now **B** becomes active.
5. Ensure **B** is handling traffic.

8

HA WUI Options

See below for descriptions of the various HA-related fields in the LoadMaster WUI.

Related Links

For details, see the following topics:

- Partner Communications
- HA and Clustering

Partner Communications



The **Partner Shared Secret** is required to secure communications between partner devices and must be enabled on all High Availability (HA) partners, all LoadMasters in a cluster, and all GEO partners. The **Partner Shared Secret** must be the same on:

- Both units in a HA setup
- All units in a LoadMaster cluster
- All GEO partners

- All remote GEO machines that retrieve Virtual Services from this device

When an incoming shared secret does not match the local **Partner Shared Secret** (including if only one side is providing a shared secret), a warn-level log message is recorded that says **Unauthorized Remote Machine connection from <ClientIPAddress>** and the connection fails.

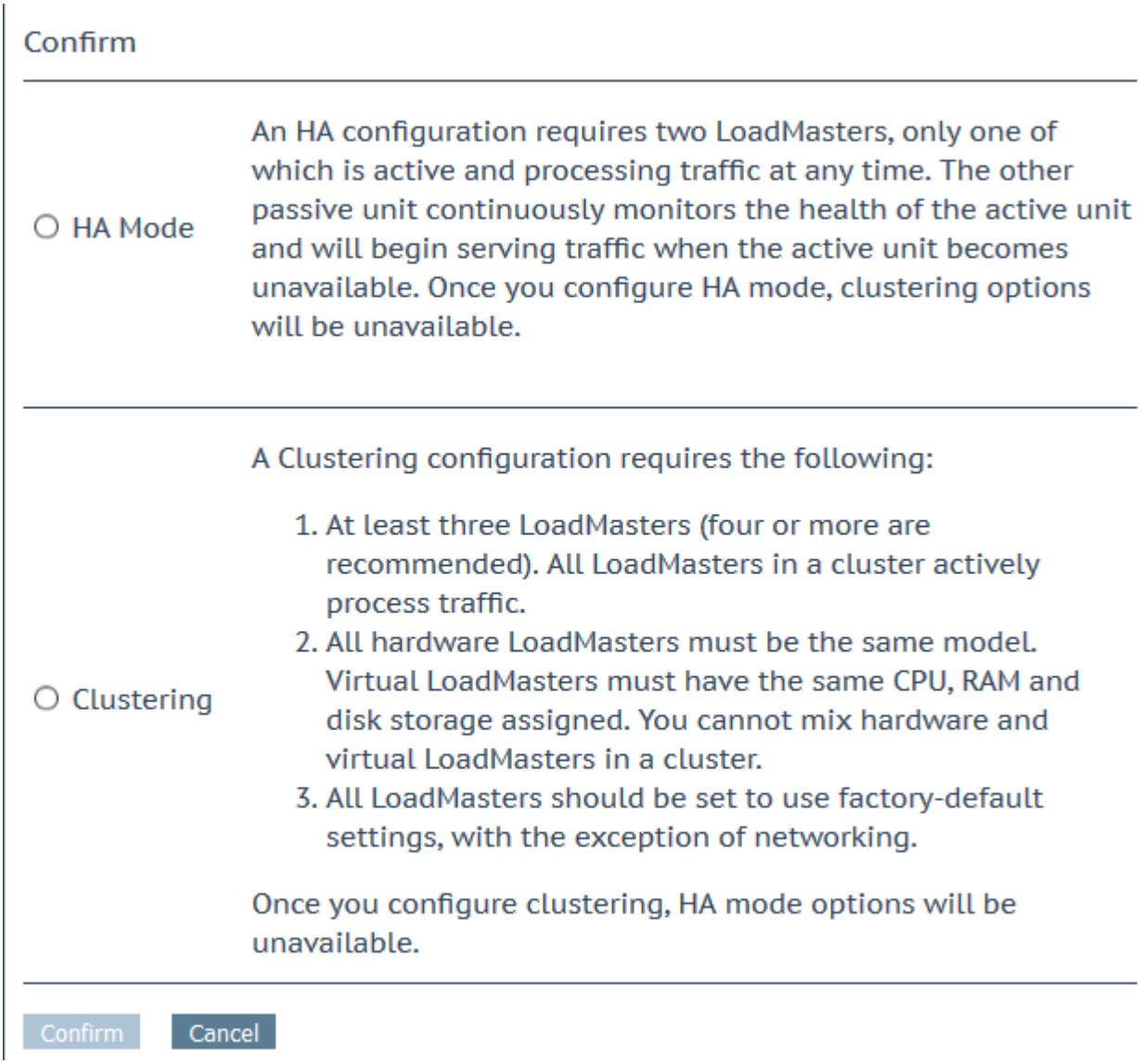
You can find this secret in the following locations:

- Regular/shared Web User Interface (WUI): **Certificates & Security > Remote Access**
- Local WUI (of a configured HA or cluster unit): **Local Administration > Remote Access**

This secret must have a minimum of 8 and a maximum of 127 characters. The following characters are supported:

- Numeric: 0-9
- Uppercase alphabetic: A-Z
- Lowercase alphabetic: a-z
- Special characters: !"#$%&()*+,-./:;<=>?[\~]^_@`{|}

HA and Clustering



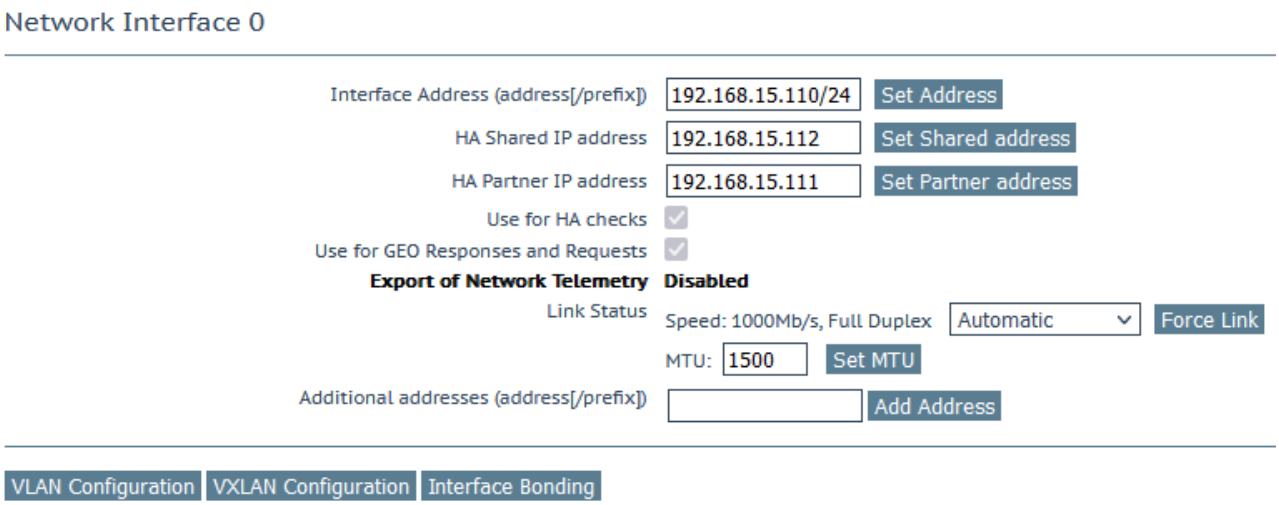
The HA section in the WUI is called **HA and Clustering**.

This screen describes both **HA Mode** and **Clustering**. Select the relevant option and click **Confirm** to continue.

Note: If clustering is configured, the HA mode options become unavailable.

Interfaces

If the unit is part of a HA configuration, the following screen displays when you click one of the interfaces.



This screen tells the user:

- The IP address of this LoadMaster (**192.168.15.110** in this example).
- The HA shared IP address (**192.168.15.112** in this example). This is the IP address used to configure the pair.
- The IP address of the paired machine (**192.168.15.111** in this example).
- Whether or not this interface is enabled for HA health-checking.
- The speed of the link (automatically detected). If the link is down, it is indicated here.
- Any alternate addresses on this interface.

Use for HA checks

Some key points to note about this option are below:

- The **Use for HA checks** check box must be selected on at least one interface that has connectivity from HA1 to HA2.
- If the **Use for HA checks** check box is grayed out it means that this is the only interface configured to be used for HA checks and cannot be deselected.
- The **Use for HA checks** option must be enabled on all production interfaces. If HA checks are only selected for non-production interfaces, the backup unit does not notice if a production interface goes down and does not switch to the active role.
- Enabling **Use for HA checks** on an interface that is directly cabled between the two units is no longer supported.

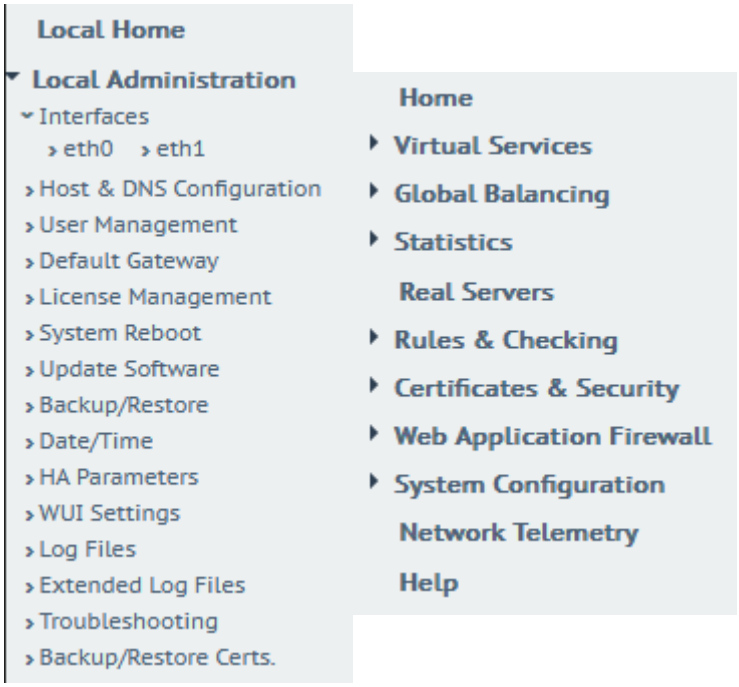
HA Parameters

You can change the role of the LoadMaster by setting the **HA Mode**. If the **HA Mode** is set **to HA (First) Mode** or **HA (Second) Mode**, a prompt appears reminding you to add a shared IP. Changing the HA Mode requires a reboot. After the details are set, click **Reboot**. Once the LoadMaster has rebooted, the **HA Parameters** menu option is available in the **System Configuration** section provided the role is not **Non HA Mode**. Configuring both units in the same **HA Mode**, for example, **HA (First Mode)** and **HA (First) Mode**,

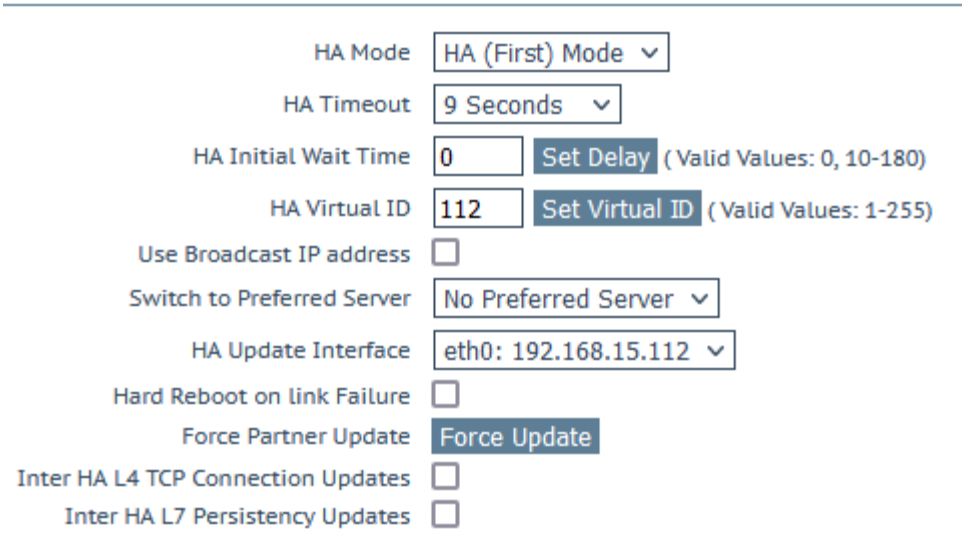
results in severe operational problems because; not only will both units be active, both units try to use the same IP address.

When logging in to the HA pair, use the shared IP address to view and set the full functionality of the pair, apart from passwords and licensing. Logging in to the direct IP address of either one of the devices displays different menu options (see menus below). Logging into one of the LoadMasters directly is usually reserved for maintenance.

After upgrading from firmware version 7.1-24b or below, if using the FIPS cavium card 1610 FW 2.2 and the LoadMaster is in HA mode, regenerate the web server SSL key to access the WUIs of the individual LoadMasters.



When a LoadMaster is in HA mode, the following screen appears when the **HA Parameters** menu option is selected:



Note: After initial configuration, the HA parameters should not be modified unless both units in the HA pair are available and operating properly (if they are both showing green icons at the top of the WUI, with one LoadMaster in active mode and the other in standby).

HA Status

At the top of the screen, next to the time, icons denote the real-time status of the LoadMaster units in the pair. There is an icon for each unit in the pair. This status is maintained using an automatic ping between the units.



Clicking these icons opens the management interface of the relevant HA partner.

The possible icons are:

Green (with 'A')		The unit is online and operational and the HA units are correctly paired. The A in the middle of the square indicates that this is the active unit.
Green (without 'A')		The unit is online and operational and the HA units are correctly paired. The absence of an 'A' in the middle of the square indicates that this is not the active unit (standby).

Red/Yellow		The partner unit is unreachable or turned off. It may be offline or misconfigured. The unit is not ready to take over. It may be offline or incorrectly paired.
Blue		When the unit reboots more than three times in 5 minutes it enters a pacified state. In this state the machine is only accessible using the direct machine WUI (not the shared WUI) and it is not participating in any HA activity. Therefore, no changes from the active unit are received and it does not take over if the active unit fails. To remove the unit from the pacified state, fix the root cause of the health check failures, log in to the pacified LoadMaster through SSH or the console and reboot. If a unit continuously reverts to a pacified state, check the network to see if CARP is being blocked.
Gray		The machine is in an indeterminate state and may require a reboot to return to operation. A gray box often means the unit has not been set up in HA mode correctly. A gray box also appears for a few seconds during the initial HA configuration. In some cases, it may mean both machines are active, that is, both are set to active, and something has gone seriously wrong.
Question marks		The HA status is updating.
Both green (left box with 'A')		Both units are up, unit 1 is active (A) and unit 2 is standby.
Both green (right box with 'A')		Both units are up, unit 1 is standby and unit 2 is active (A).
Left box green, right box red/yellow		Unit 1 is up and currently active (A). Unit 1 cannot reach unit 2, or unit 2 is turned off.

Left box red/yellow, right box green		Unit 2 is up and currently active (A). Unit 2 cannot reach unit 1, or unit 1 is turned off.
Left box gray, right box red/yellow		HA setup is not complete on unit 1.
Left box red/yellow, right box gray		HA setup is not complete on unit 2.
No HA icons		If the HA status squares are not appearing in the WUI, it probably means that HA is not enabled. Go to **System Administration** and select the HA option. Ensure the **HA Mode** is set to either **First** or **Second**.

In HA mode, each LoadMaster has its own IP address that is used only for diagnostic purposes directly on the unit. The HA pair have a shared IP address over which the WUI is used to configure and manage the pair as a single entity.

Note: There are a number of prerequisites that must be in place for HA to function correctly. Refer to the Prerequisites section for a list of these prerequisites.

HA Mode

If using a single LoadMaster, select **NonHA Mode**. When setting up HA mode, one LoadMaster must be set to **HA (First) Mode** and the other **HA (Second) Mode**. HA does not operate if both units have the same **HA Mode**.

HA Timeout

CARP requests are sent every second from the active unit. The value selected in the **HA Timeout** drop-down list is the time that the active machine must be unavailable before a switchover occurs. With this option, the time it takes a HA pair to detect a failure can be adjusted from 3 seconds to 15 seconds in 3-second increments. The default value is 9 seconds. A lower value detects failures sooner, whereas a higher value prevents HA from failing over too soon if there is a delay when receiving CARP.

To set this option, follow the steps below:

1. Select **System Configuration > HA Parameters**.
2. Select the preferred value in the **HA Timeout** drop-down list.

HA Initial Wait Time

The **HA Initial Wait Time** is the length of time after the initial boot of a LoadMaster, before the machine decides that it should become active. If the partner machine is running, this value is ignored. You can change this value to mitigate the time taken for some intelligent switches to detect that the LoadMaster has started and to bring up the link.

HA Virtual ID

When using multiple HA LoadMaster pairs (or other devices using CARP-like protocols) on the same

network, this value uniquely identifies each HA pair so that there are no potential unwanted interactions.

We highly recommend using a higher value than 10 because any other HA pair using the same ID could interfere with HA operations.

As of the 7.2.36 release, the LoadMaster selects a virtual ID based on the shared IP address of the first configured interface (the last eight bits). It is selected and displayed once both the shared address and the partner address are set. You can change the value to whatever you want (in the range 1 – 255) or you can keep it at the value it already selected. Ensure the virtual ID is unique on each LoadMaster on the network.

You can find the **HA Virtual ID** in the LoadMaster WUI by going to **System Configuration > HA Parameters**.

Use Broadcast IP address

By default, the LoadMaster uses an IP multicast address (224.0.0.18) when sending CARP packets. Enabling this option forces the use of the IP broadcast address (255.255.255.255) instead.

Switch to Preferred Server

By default, neither partner in a HA pair has priority. When a machine restarts after a failover, the machine becomes the standby and stays in that state until it is forced to active. Specifying a preferred host means that when this machine restarts, it always tries to become active and the partner reverts to standby mode.

When set to **Prefer First HA**, if the LoadMaster fails over, the active reverts to HA1 when HA1 comes back online.

When set to **Prefer Second HA**, if the LoadMaster fails over, the active reverts to HA2 when HA2 comes back online.

When **No Preferred Host** is selected, if there is a failover on the LoadMaster, the unit that becomes active remains as active (failback does not happen).

To change this option, follow the steps below in the LoadMaster WUI:

1. In the main menu, select **Local Administration > HA Parameters**.
2. Select the relevant option from the **Switch to Preferred Server** drop-down list.

Note: Some connections may be dropped during the switchover if a preferred host is specified.

For normal operating conditions, we recommend selecting **No Preferred Host**.

HA Update Interface

The interface used to synchronize the entire HA configuration within the HA pair. Synchronization occurs every two minutes. The information is synchronized over SSH port 6973.

Hard Reboot on link Failure

In LoadMaster firmware version 7.2.53, a new option, **Hard Reboot on link Failure**, was introduced. When the **Hard Reboot on link Failure** check box is enabled, the LoadMaster configured in HA reboots if any configured interface loses connectivity with the network (that is, experiences a link failure). The reboot occurs regardless of the LoadMaster's HA status (Primary or Standby).

The **Hard Reboot on link Failure** check box is available in the **System Configuration > HA Parameters** screen when both of these are true:

- High Availability (HA) is configured
- The **Switch to Preferred Server** option is set to **No Preferred Server**.

Note: The **Hard Reboot on link Failure** check box will be unavailable, if you select a preferred server from the **Switch to Preferred Server** drop-down list.

You cannot have a preferred server if **Hard Reboot on link Failure** is enabled - if you did, it could lead to circular swapping between the active and standby LoadMaster units.

Force Partner Update

Immediately forces the configuration from the active to standby unit without waiting for a normal update. This option is only available if both units can see each other in an active/standby scenario.

Inter HA L4 TCP Connection Updates

When using L4 services, enabling the **Inter HA L4 TCP Connection Updates** option allows L4 connection information to be shared between the HA partners. If a failover occurs, the connection information will be available on the unit that assumes the active role. This option does not apply to L7 services.

Note: If you do not allow multicast on the specific interface, inter-HA updates will not work. If you must have inter-HA updates, ensure to have a dedicated multicast-enabled interface for this purpose.

Inter HA L7 Persistency Updates

When a failover occurs, all connections are dropped. Enabling the **Inter HA L7 Persistency Updates** option can help to send some traffic back to the same Real Server, but the connections are still dropped after a failover.

When using L7 services, enabling the **Inter HA L7 Persistency Updates** option allows L7 persistence information to be shared between the HA partners. If a failover occurs, the persistence information will be available on the unit that assumes the active role. This option does not apply to L4 services.

Note: Enabling this option can have a significant performance impact.

Note: If you do not allow multicast on the specific interface, inter-HA updates will not work. If you must have inter-HA updates, ensure to have a dedicated multicast-enabled interface for this purpose.

HA Multicast Interface

The network interface used for multicast traffic, which is used to synchronize Layer 4 and Layer 7 traffic when Inter HA Updates are enabled.

You can select the interface to send and receive inter-HA traffic from within the WUI of the shared IP address:

1. In the main menu, select **System Configuration > HA Parameters**.

2. The **HA Update Interface** setting is used for sending HA configuration updates using TCP/6973 between units. Modify it if needed.

If you have enabled L7 persistency updates or L4 TCP connection updates, an additional **HA Multicast Interface** option also becomes available.

Use Virtual MAC Addresses

Selecting this option creates a shared MAC address for both units. When failover occurs, the LoadMaster handles the MAC address handover too. This allows the switches to keep the same MAC address and not worry about ARP caches or stale records. This is useful when gratuitous ARPs (used in communicating changes in HA IP addresses to switches) are not allowed.

Virtual MAC (VMAC) is a way of doing HA at Layer 2, rather than Layer 3. In addition to a shared IP address, there is a shared MAC address that is owned by whichever unit is active. By implementing this, all Virtual Service traffic communicates to this shared MAC address, allowing the standby device to pick up the traffic seamlessly. In the event of a failover, upstream devices do not need to change the Address Redundancy Protocol (ARP) record associated with the services. The only change that must occur is that the switch must begin sending frames out a different port.

VMAC is the best way to accomplish HA. The only reason it is not defaulted is because some environments prohibit migrating MAC addresses across ports. Settings such as Cisco's Port Security can prevent VMAC from working properly.

A quick way to test whether your environment can use this is the 'laptop test'. To do the 'laptop test', follow the steps below:

1. Get a laptop and plug it into a port on the switch.
2. Get connectivity.
3. Move the connection to a different port on the same switch.

If connectivity returns without incident, then you should also be able to use VMAC.

If your HA pair is connected to two different switches, the laptop test should be done on the switch that those switches converge at (rather than the switches the LoadMaster connects to) because that is where the MAC bookkeeping has to change quickly.

After confirming that VMAC will work in your environment, you can change to Virtual MAC during a maintenance window because it requires a reboot. Also, ARP must be flushed on relevant devices. To turn it on, select the **Use Virtual MAC addresses** check box in the LoadMaster WUI by going to **Local Administration > HA Parameters** on both devices. Following that, you must reboot both devices. You also must flush the ARP on all upstream devices. It is recommended, but may not be necessary, to also flush ARP on the Real Servers.

Note: This option is not available in Virtual or Cloud LoadMasters because they are not physically connected.

This is the expected behavior when Virtual MAC (VMAC) is enabled and a fail-over occurs:

IP address	MAC address	Type	Unit
192.168.15.111	00-10-f3-19-31-26	dynamic	Standby unit
192.168.15.110	00-00-5e-00-01-48	dynamic	Master unit
192.168.15.112	00-00-5e-00-01-48	dynamic	Shared IP

Following a fail-over:

IP address	MAC address	Type	Unit
192.168.15.111	00-00-5e-00-01-48	dynamic	New master
192.168.15.110	00-10-f3-18-d4-82	dynamic	New standby
192.168.15.112	00-00-5e-00-01-48	dynamic	Shared IP

Here is the expected behavior without VMAC enabled:

IP address	MAC address	Type	Unit
192.168.15.111	00-10-f3-19-31-26	dynamic	Standby unit
192.168.15.110	00-10-f3-18-d4-82	dynamic	Master unit
192.168.15.112	00-10-f3-18-d4-82	dynamic	Shared IP

Following a fail-over:

IP address	MAC address	Type	Unit
192.168.15.111	00-10-f3-19-31-26	dynamic	New master
192.168.15.110	00-10-f3-18-d4-82	dynamic	New standby
192.168.15.112	00-10-f3-19-31-26	dynamic	Shared IP

Switches may not update their ARP table to reflect the change in fail-over.

The switch sends traffic to 192.168.11.245 (00-10-f3-18-d4-82 (Standby unit)).

9

Troubleshooting

This section outlines troubleshooting steps for some common HA-related problems. If further help is needed, contact Progress Kemp Support.

Related Links

For details, see the following topics:

- General Troubleshooting Tips
- Confirm Settings
- No HA Status Squares are Visible in the WUI
- Green/Red HA Status Squares
- Blue HA Status Square
- Both Units are Active and the WUI is Unresponsive - Blue or Red Status Square
- Gray HA Status Square
- Virtual Services Temporarily Unavailable After Failover
- No Access to WUI on HA1/2 or Shared
- Nothing Works
- Issue with Hyper-V and HA on a Pair of VLMs
- Synchronization Issue After Unbonding/Bonding an Interface

- Log Messages Explanations

General Troubleshooting Tips

General HA troubleshooting steps are below:

- Check that the IP settings for the **Interface**, **Partner**, and **Shared IP address** are correct. These settings can be found in **System Configuration > Interfaces**.
- A shared IP address must be added to all production interfaces.
- The **Use for HA checks** option must be enabled on all production interfaces.
- Log in to each of the single HA interface addresses and ensure the HA parameters are correct (**Local Administration > HA Parameters**):
  - Ensure that the HA pair has one unit in **HA (First) Mode** and another unit in **HA (Second) Mode**.
  - Ensure that both units are on the same protocol and HA ID.
- Ensure that all of the IP addresses are available and are not in use by another device. IP conflict causes numerous problems.
- Shut down one or both LoadMasters and try to ping the IP address of each unit. If there is an answer, another device is using that IP address. Try the 'arp -a' or 'netstat' commands to find out more information on what device that is.
- Set the **HA Virtual ID** (in **Local Administration > HA Parameters**) to something other than **1**. The further up the range the better – avoid numbers from 1 to 10 because other HA pairs may have those IDs and use Virtual Router Redundancy Protocol (VRRP).

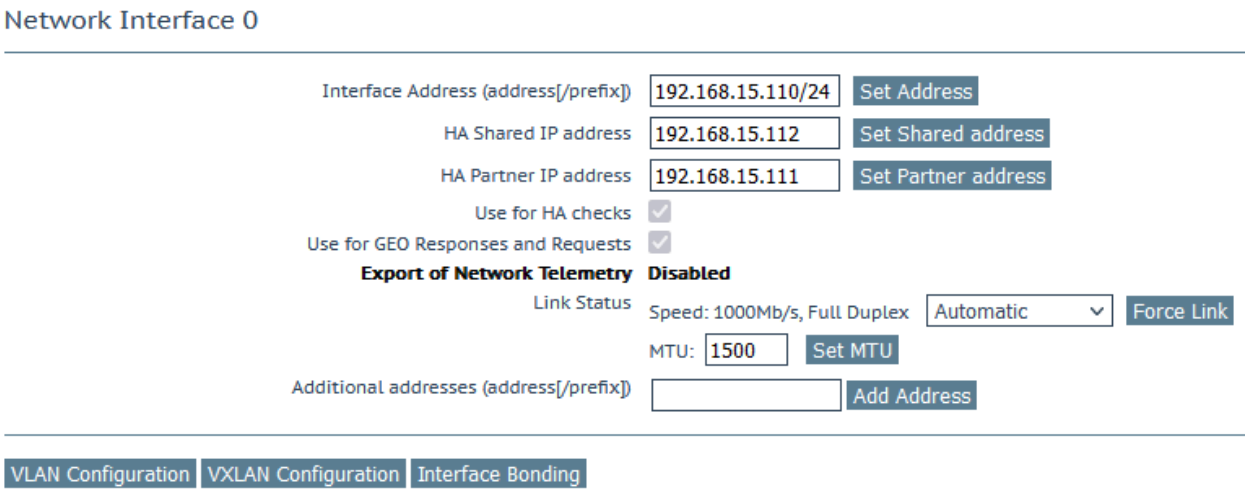
Note: The Virtual ID can conflict with any device on the network which is using VRRP. If there are multiple HA pairs on the same network, they must also have different Virtual IDs.

- Check that the time of both units are in sync and if they are not, ensure that NTP is configured and running on both units.
- Ensure there are no Virtual Services using TCP and port 6973 on the interface where synchronization is configured.
- Ensure there are no Virtual Services on either of the HA individual addresses.
- Ensure there are no Virtual Services using TCP and port 22 on a LoadMaster interface port.

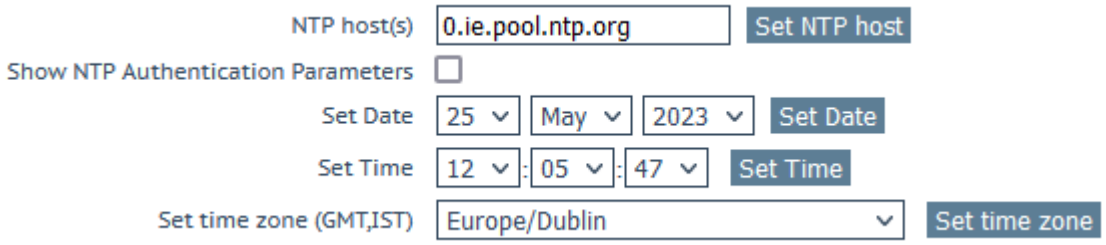
Confirm Settings

If you are experiencing problems with HA, confirm that:

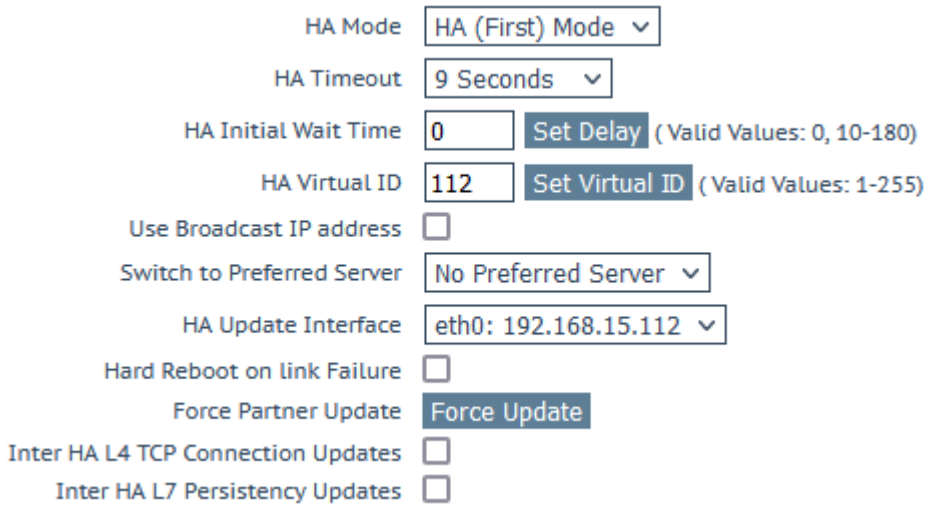
- The **Partner Shared Secret** matches in both the active and standby unit. You can find this secret in the following locations:
  - Regular/shared WUI: **Certificates & Security > Remote Access**
  - Local WUI (of a configured HA unit): **Local Administration > Remote Access**
- The two LoadMasters are on the same subnet.



- For each Network Interface Card (NIC) that has **Use for HA checks** enabled, the link status shows as connected.
- The two units can ping each other and their default gateway. (The ping options are available in **System Configuration > Troubleshooting**.)



- Both units have the same time. Set both units to use the same NTP server and correct time zone. (The date and time options are available in **Local Administration > Date/Time**).



- Unit 1 is set to **HA (First) Mode**.Unit 2 is set to **HA (Second) Mode**.The **HA Virtual ID** is the same on both units.

In terms of the network switch settings:

- Confirm that Promiscuous mode and PortFast are enabled.
- If HA is configured for multicast traffic (that is, if **Use Broadcast IP address** is disabled on the LoadMaster **HA Parameters** screen), then:
  - Confirm that the switch allows multicast traffic
  - Confirm that settings that block multicast traffic, such as 'IGMP snooping', are disabled on the switch.

Sometimes there are logs relating to HA, such as:

```
<date> <LoadMasterHostName> ucarp[2193]: Bad digest - md2=[xxxxx...]
md=[xxxxx...]

- Check vhid, password and virtual IP address
```

For example:

```
Jul 13 17:47:10 Kemp_1 ucarp[2193]: Bad digest - md2=[31084da3...]
md=[20dcd914...] - Check vhid, password and virtual IP address
```

The most common reasons for this error are as follows:

- There is another device on the network with the same HA Virtual ID. The LoadMasters in a HA pair should have the same HA Virtual ID. It is possible that a third device could be interfering with these units. As of LoadMaster firmware version 7.2.36, the LoadMaster selects a HA Virtual ID based on the shared IP address of the first configured interface (the last 8 bits). You can change the value to whatever number you want (in the range 1 - 255), or you can keep it at the value already selected.
- An interface used for HA checks is receiving a packet from a different interface/appliance. If the LoadMaster has two interfaces connecting to the same switch, with **Use for HA checks** enabled, this can also cause these error messages. Disable the **Use for HA checks** option on one of the interfaces to confirm the issue. If confirmed, either leave the option disabled, or move the interface to a separate switch.

Further Details about IGMP Snooping and PortFast

IGMP Snooping

If Internet Group Management Protocol (IGMP) snooping is enabled, this can cause issues when HA is configured to use multicast packets (the default). With IGMP enabled, the switch intelligently detects which hosts belong to a multicast to restrict the number of hosts that receive the multicast. Typically it does not detect LoadMaster multicasts correctly. This can lead to one of two situations - either CARP packets flow one way or they do not flow at all. This is why we recommend disabling IGMP snooping when using HA with multicast CARP packets. (IGMP has no effect when using HA with broadcast CARP packets.).

PortFast

If you do not have PortFast enabled, the following issues may occur:

- The LoadMaster shows as Active/Active after one unit is rebooted
- The LoadMaster (LM1) allows a failover to the passive LoadMaster (LM2). When the port comes back up, LM1 takes over as active even when no preferred active is set.

When you enable PortFast on the switch, the spanning tree places ports in the forwarding state immediately, instead of going through the listening, learning, and forwarding states. By default, the spanning tree sends Bridge Protocol Data Units (BPDUs) from all ports regardless of whether PostFast is enabled.

Having PostFast enabled on a switch that the LoadMaster is directly connected to is advisable. If a port goes down, the LoadMaster is aware right away otherwise it performs the three states.

After the changes on the vSwitch, if there is still an Active-Active state, it means the LoadMasters are on separate hosts and switch setup must be performed on the hardware switch.

No HA Status Squares are Visible in the WUI



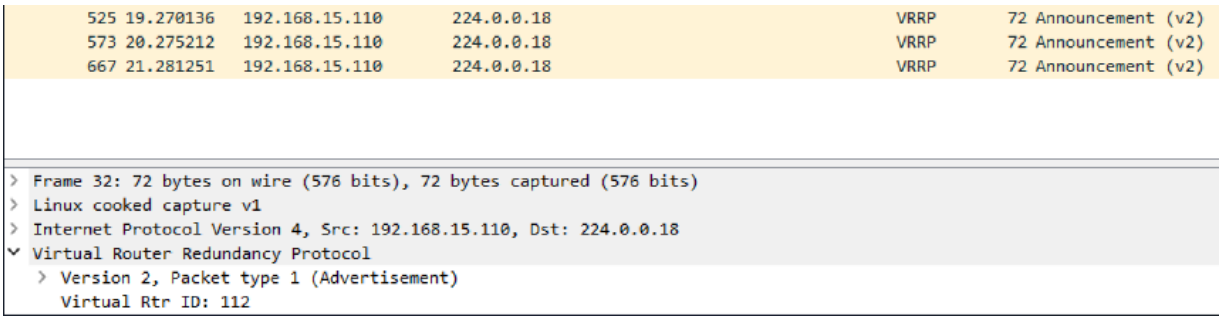
If the HA status squares are not appearing in the WUI, it may mean that HA is not enabled. Go to **System Administration > HA Parameters** and ensure the **HA Mode** is set to either **First** or **Second**.

Green/Red HA Status Squares

If one of the HA status squares is red, check if one of the machines has crashed. If it has not crashed, try the following steps:

- If HA is configured for multicast traffic (that is, if **Use Broadcast IP address** is disabled on the LoadMaster **HA Parameters** screen), then:
  - Confirm that the switch allows multicast traffic.
  - Confirm that settings that block multicast traffic, such as 'IGMP snooping', are disabled on the switch.
- Ensure that promiscuous mode and portfast is enabled on the switch(es) connecting both units.
- For Virtual LoadMasters (VLMs);
  - Ensure that MAC spoofing is allowed.
  - Move both units to the same host to confirm the issue is related to hardware devices/switches.
  - In VMware - ensure **Notify Switches** is set to **No**.
  - In VMware, there are security policies that can be applied to the virtual switches that can prevent a Virtual LoadMaster from properly controlling the MAC addresses for HA. You can find out more about these policies by referring to the VMware documentation.
  - Hyper-V has a per-vNIC setting to **Allow MAC Spoofing** in the Virtual Machine NIC settings - this must be enabled. This can be enabled in the Hyper-V Manager Graphical User Interface (GUI) or using PowerShell. Refer to the Microsoft documentation for further information.
- Reboot both of the units using a single IP.
- Ping between the units.
- Confirm the IP address settings.
- Check the HA settings on both machines.
- Select more than one interface for HA checks.

- For hardware LoadMasters;
  - Enabling **Use for HA checks** on an interface that is directly cabled between the two units is no longer supported.
  - Check that **No Preferred Host** is selected in the **Switch to Preferred Server** field. If HA works when you do this, the network could be the issue.



  - Run a TCP dump on unit 2. The source IP address should be the IP address of the interface. The destination IP address should be either a multicast address (224.0.0.18) or the broadcast address (255.255.255.255) if **Use Broadcast IP address** is enabled. Check that the Virtual Host ID is correct (in the above example the Virtual Host Id is 112). If no VRRP packets are seen and multicast CARP is enabled, multicast may be blocked on the switch or IGMP snooping may be enabled.

- Change the **HA Virtual ID** to something other than 1 (preferably higher than 10).
- Increase the value of the HA timeouts.

Blue HA Status Square

If there is a blue HA status square, follow the steps below:

1. Let the affected unit run for 10 minutes.

   Note: While waiting you can check the HA parameters to ensure they are configured correctly.

2. After that, shut down the blue unit for 5 minutes and restart using SSH or the console.
3. Confirm the network and HA settings.

Both Units are Active and the WUI is Unresponsive - Blue or Red Status Square

This usually means that both units are set to the same **HA Mode**, for example **HA (First) Mode**. This causes both units to be active and to try to take the same IP address. This causes serious problems with all functions of the LoadMaster.

Gray HA Status Square

A gray HA status square usually indicates that the unit has not been set up in HA mode correctly. A gray square is expected for a few seconds during initial HA setup.

Virtual Services Temporarily Unavailable After Failover

If Virtual Services are temporarily unavailable after a failover, try flushing the Address Resolution Protocol (ARP) cache on the next-hop Layer 3 device which the LoadMaster is connected to.

If that does not work, activate Virtual MAC and flush the ARP cache. Activating the Virtual MAC requires a reboot on both units.

Note: The Virtual MAC option is not available in Virtual or Cloud LoadMasters due to the inability to physically influence the units.

To activate Virtual MAC, follow the steps below:

1. In the shared IP address WUI, go to **System Configuration > HA Parameters**.
2. Enable the **Use Virtual MAC Addresses** option.

Selecting this option creates a shared MAC address for both units. When failover occurs, the LoadMaster handles the MAC address handover too. This allows the switches to keep the same MAC address and not worry about ARP caches or stale records. This is useful when gratuitous ARPs (used in communicating changes in HA IP addresses to switches) are not allowed.

No Access to WUI on HA1/2 or Shared

If the WUI is inaccessible using any of the three IP addresses, try the steps below:

- Wait 5 minutes and try again. Sometimes WUI access has not yet been activated, even though the LoadMaster is responding to pings.
- Try a different web browser.
- Clear the web browser cache.
- Try from a different computer.
- Log in to the console (of the IP address where the problem is occurring) using SSH, go to option **3 Local Administration**, **4 Web Address** and **s Immediately Stop Web Server Access**, which will then turn into **s Immediately Start Web Server Access**. This should restart hanging WUI access.

Nothing Works

If everything in this troubleshooting section fails, try to shut down one of the LoadMasters. The remaining LoadMaster should take over. This can remain in HA mode or be set to single – whichever works. This provides a working solution until a more permanent fix can be found.

Issue with Hyper-V and HA on a Pair of VLMs

If you are having problems with Hyper-V and HA on a pair of VLMs, you may need to configure MAC address spoofing. The following Microsoft TechNet article may help you to fix the problem: http://technet.microsoft.com/en-us/magazine/ff458341.aspx

Synchronization Issue After Unbonding/Bonding an Interface

Occasionally, after unbonding a bonded interface or bonding an unbonded interface – the active/standby units cannot communicate. To fix this issue, restart the active unit.

Log Messages Explanations

Some common HA log messages and their explanations are as follows:

Log:

```
<Time> <LoadMasterHostname> ucarp[]: Bad digest -md2=[...] md=[...] - Check
vhid, password and virtual IP address
```

Explanation

An interface used for HA checks is receiving a packet from a different interface/appliance.

How to solve

Check that the LoadMaster pair is using a unique HA-ID.

Check that an interface is not receiving packets from another interface. For example, eth0 is used for sending HA status but it is connected to the same switch as eth1. In this scenario, eth1 will see the packets and report this error message.

Log:

```
<Time> <LoadMasterHostname> ucarp[]: [WARNING] HA Config file has changed -
reloading
```

Explanation:

A user made changes to the HA parameters.

Log:

```
<Time> <LoadMasterHostname> ucarp[]: [CRITICAL] Detected Active - Active re-
arping
```

Explanation:

This message occurs when both LoadMasters become "Active". The LoadMaster that is set to "HA Mode First" (LM1) receives a CARP packet from "LM2". It detects another Active on the network, informs LM2 that the Active is up and healthy, and re-ARPs to update the routers/firewalls.

Log:

```
<Time> <LoadMaster Hostname> ucarp []: [WARNING] Bad TTL
```

Explanation:

This means the machine sending the CARP message (this might not be a LoadMaster) is not on the same network. It is at least one hop away.

Log:

```
<Time> <LoadMaster Hostname> ucarp []: [WARNING] Switching to state: Active
```

Explanation:

The connection to the partner unit has been lost or the unit is not responding correctly to CARP messages.

How to solve:

Verify that the partner unit is up and running. Follow the tips in the General Troubleshooting Tips section and confirm all switch settings per the guidelines in the Confirm Settings section.

10

Replacing Hardware HA Units

When replacing hardware HA units, it is important to follow the correct steps in sequence to ensure that there is little or no downtime for end users. The below example has two old units which are to be replaced with two new units.

The steps below are written assuming that the new units are powered on and available to be provisioned and that all cabling is in place.



Old unit 1 (A) (Active)



Old unit 2 (B) (Standby)

No preferred active set

Replacement units:

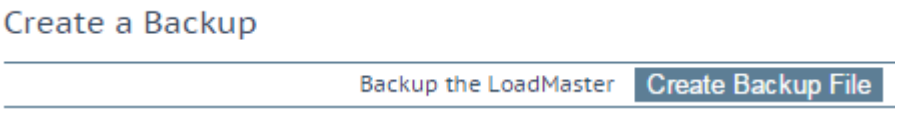


New unit 1 (C)

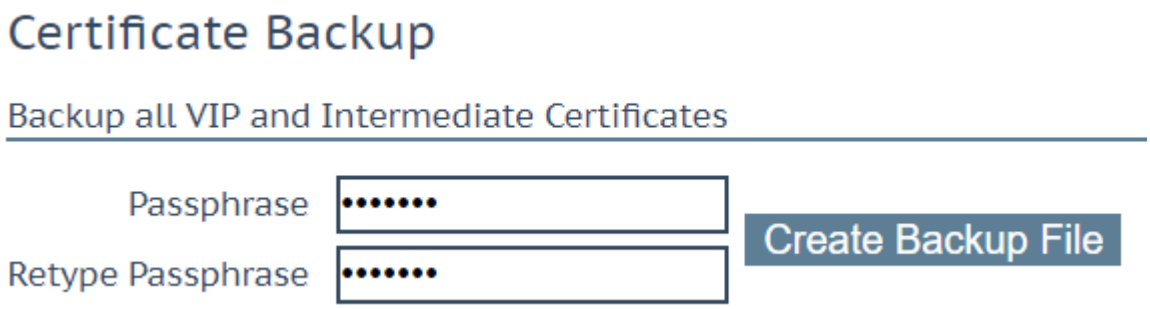


New unit 2 (D)

1. On the WUI of the individual unit being replaced, in the main menu, go to **Local Administration > Backup/Restore**.



2. Click **Create Backup File**.
3. Save the backup file.
4. In the main menu, go to **Certificates & Security > Backup/Restore Certs**.



5. Enter the same passphrase in the **Passphrase** and **Retype Passphrase** text boxes.

Note: Retain this passphrase because you need it to restore the certificates.

6. Click **Create Backup File**.
7. Remove old unit 2 (B) from production.

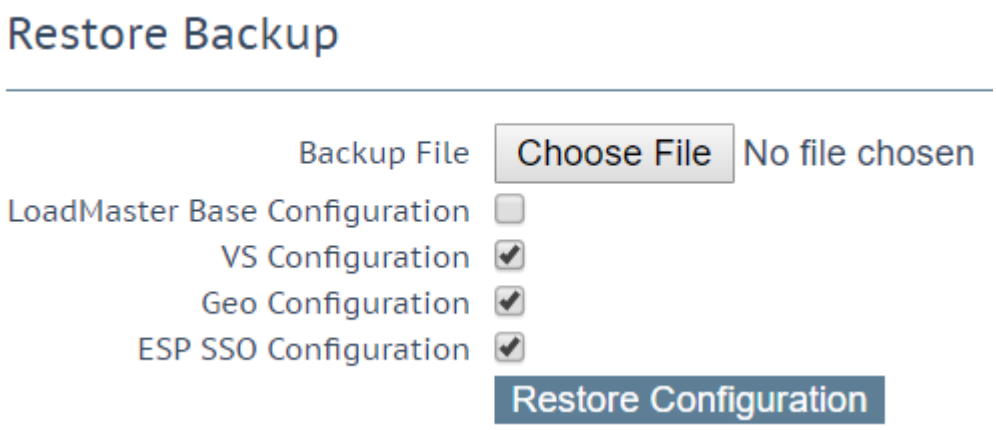
Note: As old unit 1 (A) is active, this should not affect production.

8. In the WUI of new unit 2 (D), in the main menu, go to **System Configuration > System Administration > Backup/Restore**.

Note: It is not possible to restore a configuration containing ESP-enabled Virtual Services onto a

machine which is not enabled for ESP.

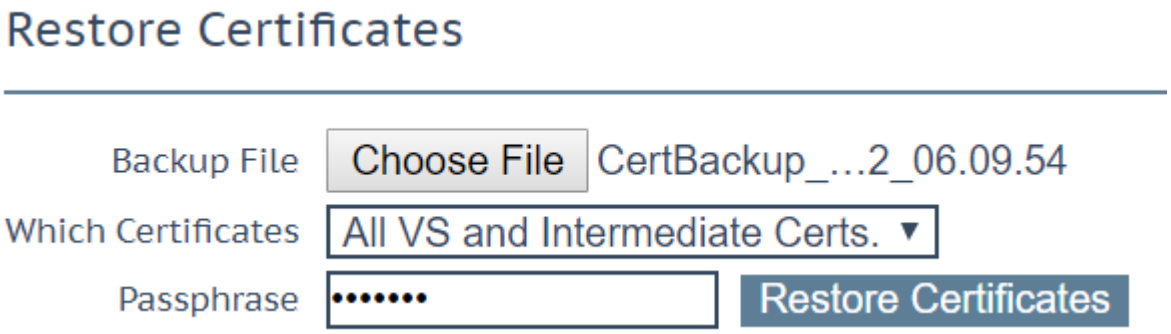
Note: You cannot restore the **LoadMaster Base Configuration** of a standalone unit to a HA pair or restore a HA configuration onto a single machine. A unit must be put into HA mode before a backup from a HA machine can be used to restore the **LoadMaster Base Configuration**.



9. Click **Choose File**.
10. Browse to and select the backup file.
11. Select the configuration(s) to be restored.

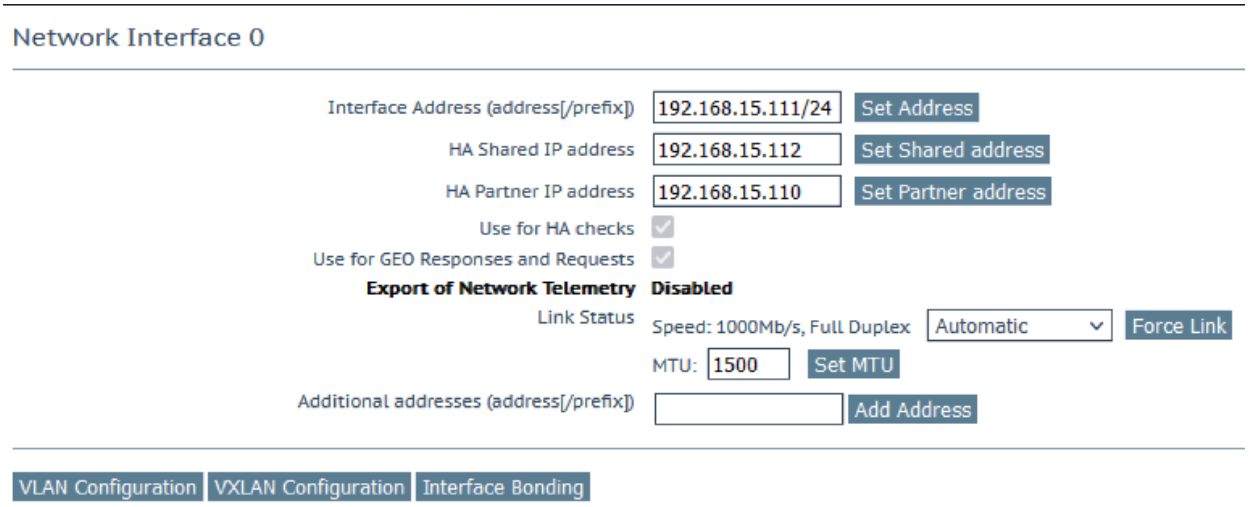
Note: This is the backup from old unit 2 (B).

12. Click **Restore Configuration**.
13. Click **Reboot Now**.
14. Click **Continue**.
15. In the main menu, go to **Certificates & Security > Backup/Restore Certs**.
16. Click **Choose File**.

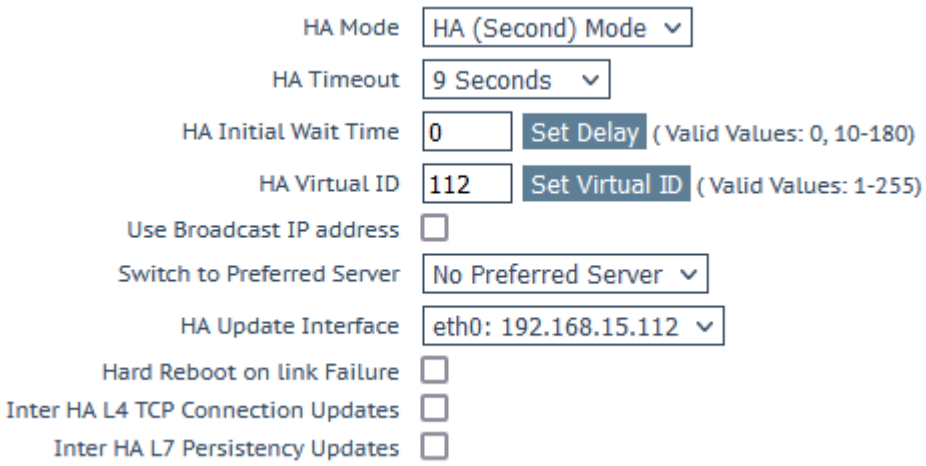


17. Browse to and select the certificate backup file.
18. Select **All VS and Intermediate Certs.**.
19. Enter the **Passphrase** which was entered when taking the certificate backup.
20. Click **Restore Certificates**.

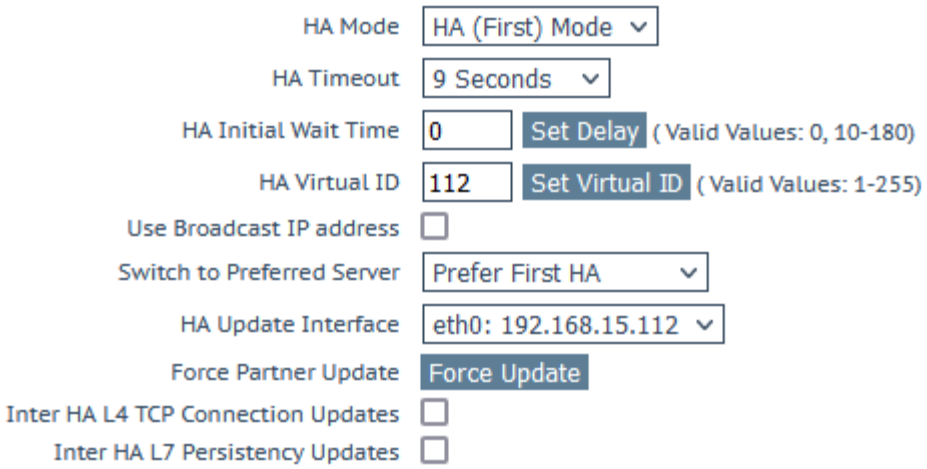
21. In the main menu, go to **Local Administration > Interfaces**.
22. Select the relevant interface.



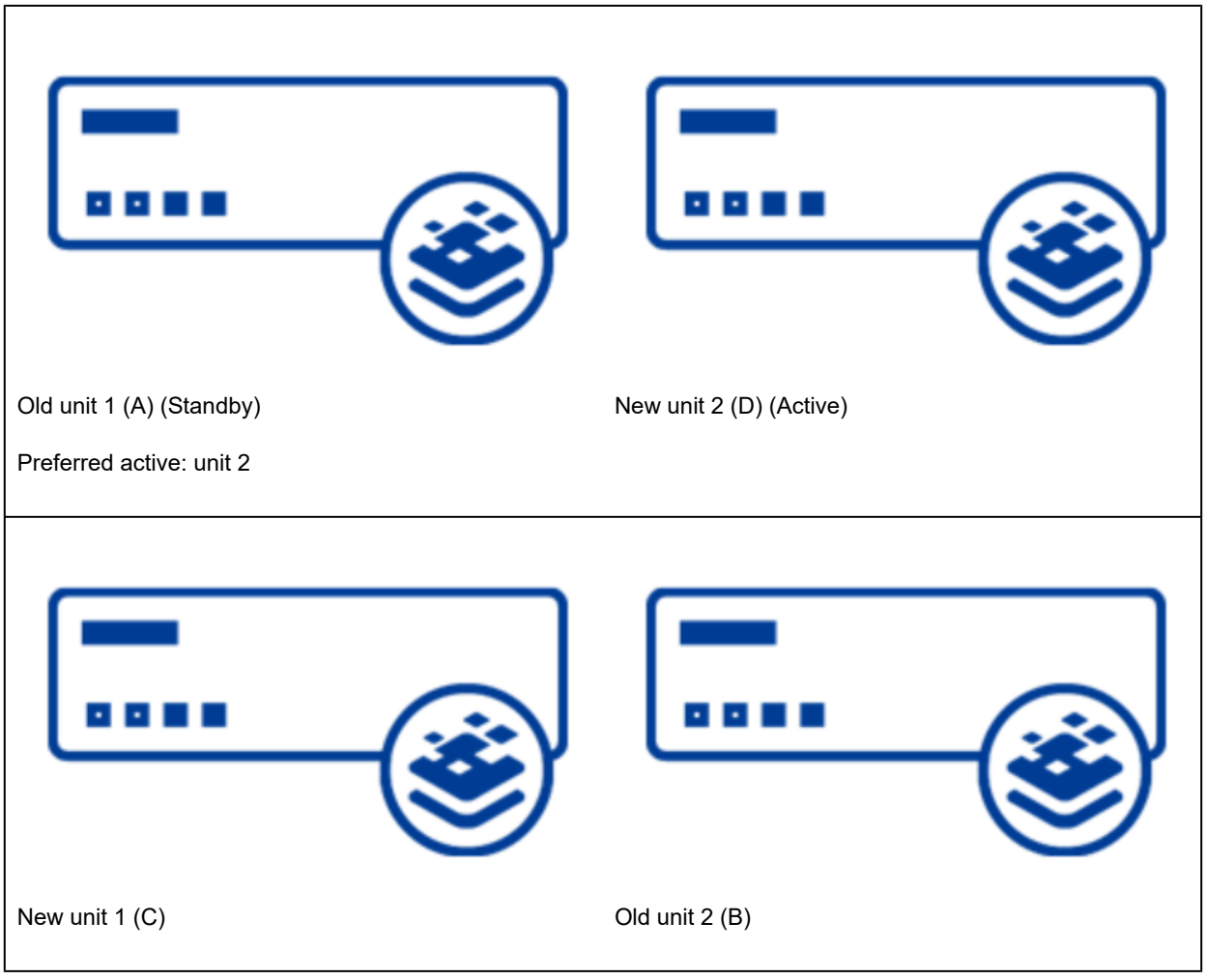
23. Check that the **Interface Address (address[/prefix])**, the **HA Shared IP address** and **HA Partner IP address** are correct before adding it to the production unit.
24. In the main menu, go to **Local Administration > HA Parameters**.



25. Ensure that the **HA Virtual ID** is correct and unique.
26. When the new unit 2 (D) is connected, open the WUI of the shared IP address and in the main menu, go to **System Configuration > HA Parameters**.



27. Click **Force Update**.

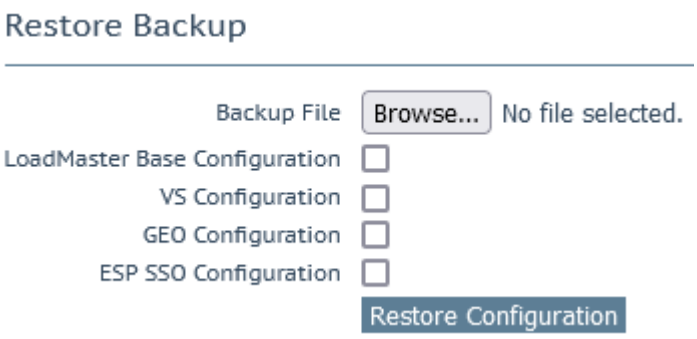


Note: This copies the configuration from the old unit 1 (A) (Master) to the new unit 2 (D) (standby). This takes approximately 15 seconds.

28. Now, old unit 1 (A) can be removed from production.

Note: As new unit 2 (D) is active, this should not affect production.

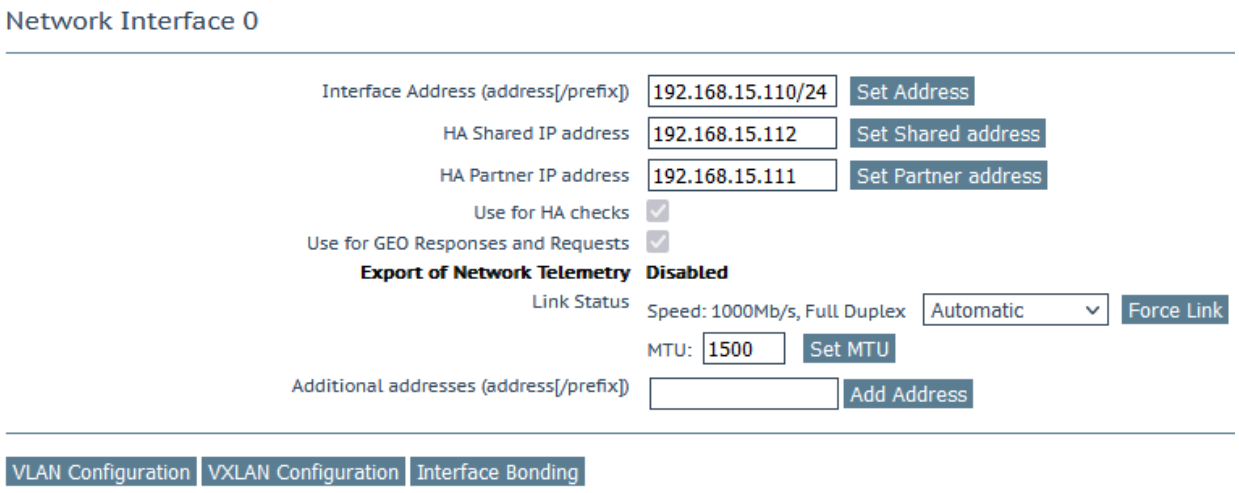
29. On the WUI of the new unit 1 (C), in the main menu, go to **System Configuration > System Administration > Backup/Restore**.



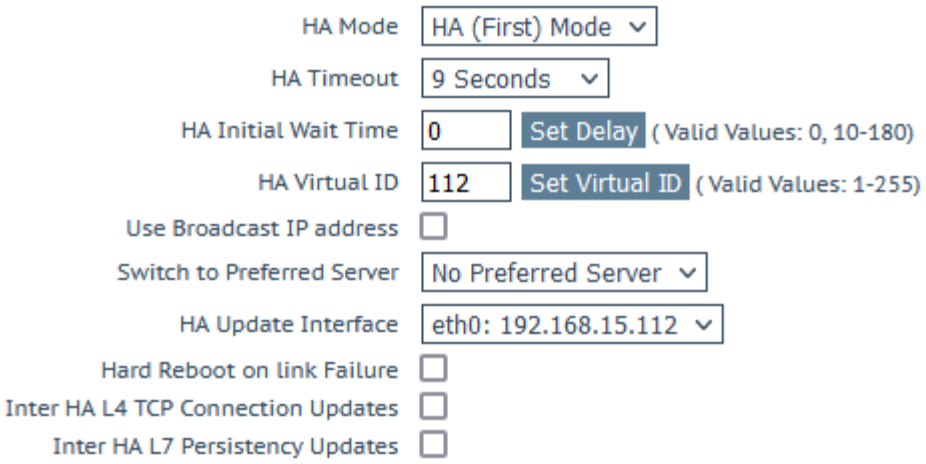
30. Click **Choose File**.
31. Browse to and select the backup file.
32. Select the configuration(s) to be restored.

Note: This is the backup configuration from old unit 1 (A).

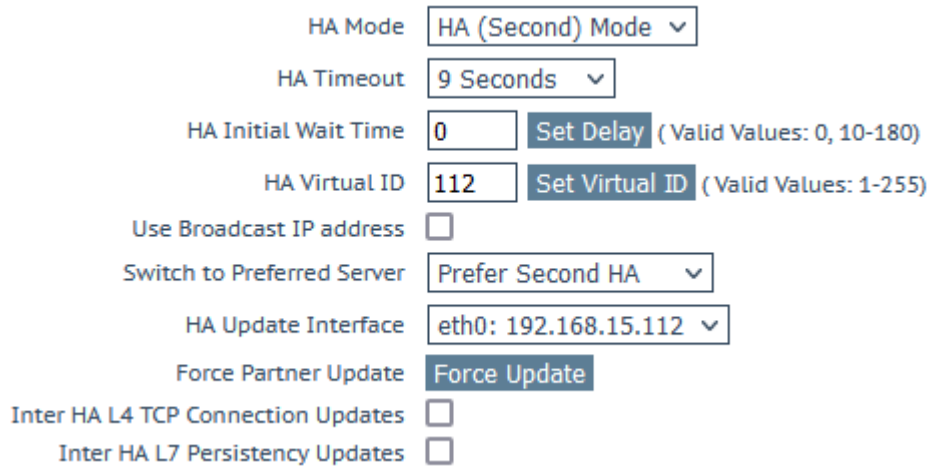
33. Click **Restore Configuration**.
34. Click **Reboot Now**.
35. Click **Continue**.
36. In the main menu, go to **Local Administration > Interfaces**.
37. Select the relevant interface.



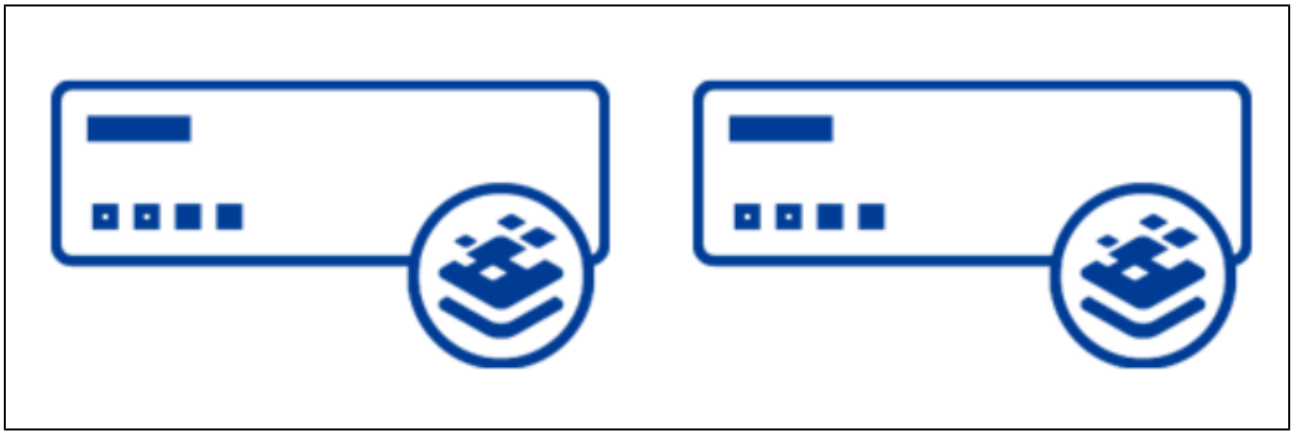
38. Check that the **Interface Address (address[/prefix])**, the **HA Shared IP address** and **HA Partner IP address** are correct before adding it to the production unit.
39. In the main menu, go to **Local Administration > HA Parameters**.



40. Ensure that the **HA Virtual ID** is correct and unique.
41. When new unit 1 (C) is connected, open the WUI of the shared IP address and in the main menu, go to **System Configuration > HA Parameters**.



42. Click **Force Update**.
43. This takes approximately 15 seconds.



New unit 1 (C) (Standby) Preferred active set to none Current setup – two units in production	New unit 2 (D) (Active)
	
Old unit 1 (A)	Old unit 2 (B)

Note: If you are replacing faulty units, ensure to send the old faulty units back to Progress Kemp for testing.

Ensure the **Partner Shared Secret** matches in both the active and standby unit. You can find this secret in the following locations:

- Regular/shared WUI: **Certificates & Security > Remote Access**
- Local WUI (of a configured HA unit): **Local Administration > Remote Access**

11

Replacing Virtual HA Units

When replacing virtual HA units, it is important to follow the correct steps in sequence to ensure that there is little or no downtime for end users.

Please verify that the Virtual Machines are configured with the recommended settings:

- When using High Availability (HA), ensure that **MAC address changes** and **Forged transmits** are both set to **Accept**. Ensure this is forced (hard coded) on the port group because any changes to the vSwitch will affect all port groups by default.

  Note: Starting with vSphere version 7.0, the default values for **MAC Address Changes** and **Forged Transmits** are set to **Reject** by default; in previous vSphere releases, these parameters were set to **Accept** by default. While it has always been a step in the VMware HA configuration process to ensure that these parameters are set to **Accept** for LoadMaster, extra care will need to be taken with vSphere version 7.0 and later releases. To mitigate against any security concerns about changing these default values, create a separate management plane subnet for LoadMaster HA using a dedicated vSwitch or separate port groups.

- When using HA and the LoadMasters are on different hosts: To prevent the transmission of RARP packets from being sent every time a Virtual Machine is powered on in a VMware environment, enable Promiscuous mode and set the **Notify Switches** option to **No**.

The below example has two old units which are to be replaced with two new units.

The steps below are written assuming the LoadMaster network cards are connected to the correct virtual switches/VLANs.



Old unit 1 (A) (Active)

No preferred active set

Replacement units:



Old unit 2 (B) (Standby)

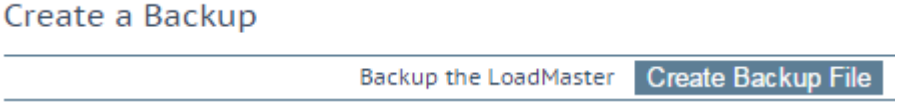


New unit 1 (C)

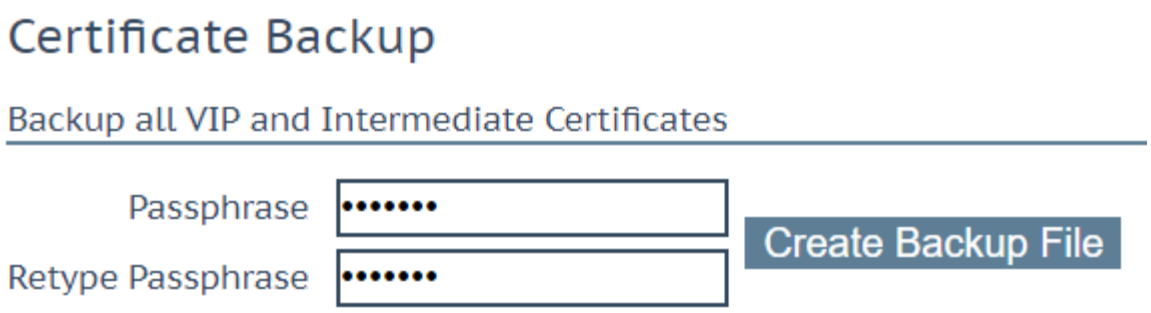


New unit 2 (D)

1. On the WUI of the individual unit being replaced, in the main menu, go to **Local Administration > Backup/Restore**.



2. Click **Create Backup File**.
3. Save the backup file.
4. In the main menu, go to **Certificates & Security > Backup/Restore Certs**.



5. Enter the same passphrase in the **Passphrase** and **Retype Passphrase** text boxes.

   Note: Retain this passphrase because you need it to restore the certificates.

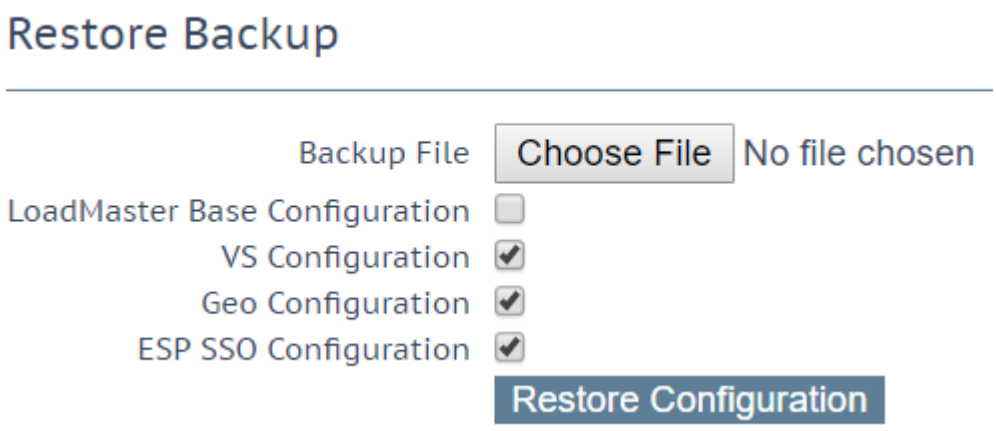
6. Click **Create Backup File**.
7. Remove old unit 2 (B) from production.

   Note: As old unit 1 (A) is active, this should not affect production.

8. In the WUI of new unit 2 (D), in the main menu, go to **System Configuration > System Administration > Backup/Restore**.

   Note: It is not possible to restore a configuration containing ESP-enabled Virtual Services onto a machine which is not enabled for ESP.

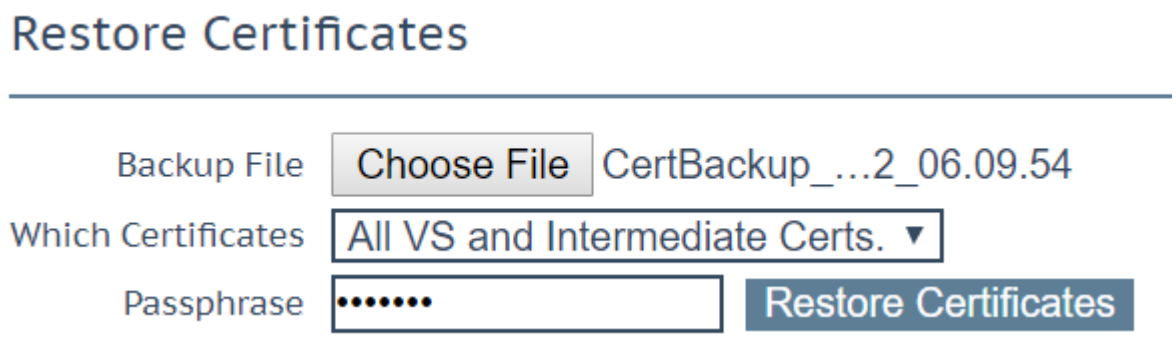
   Note: You cannot restore the **LoadMaster Base Configuration** of a standalone unit to a HA pair or restore a HA configuration onto a single machine. A unit must be put into HA mode before a backup from a HA machine can be used to restore the **LoadMaster Base Configuration**.



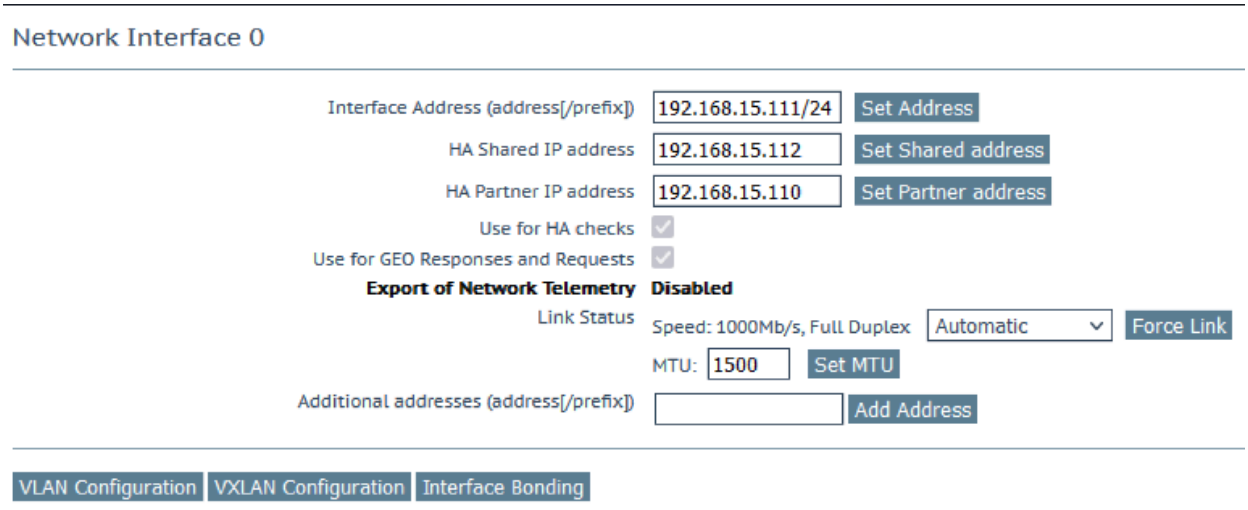
9. Click **Choose File**.
10. Browse to and select the backup file.
11. Select the configuration(s) to be restored.

    Note: This is the backup from old unit 2 (B).

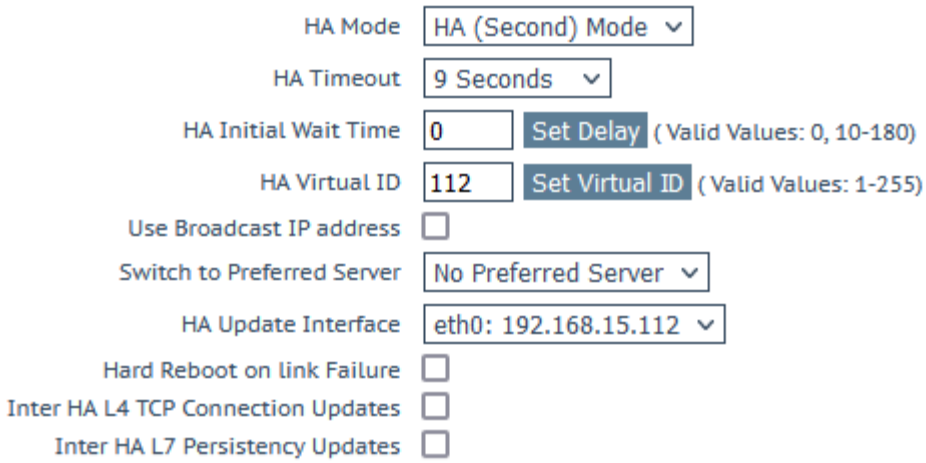
12. Click **Restore Configuration**.
13. Click **Reboot Now**.
14. Click **Continue**.
15. In the main menu, go to **Certificates & Security > Backup/Restore Certs**.
16. Click **Choose File**.



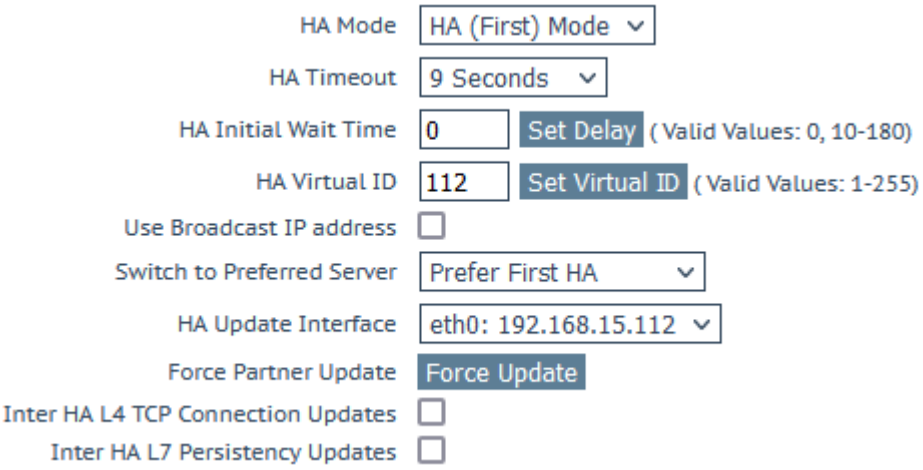
17. Browse to and select the certificate backup file.
18. Select **All VS and Intermediate Certs.**.
19. Enter the **Passphrase** which was entered when taking the certificate backup.
20. Click **Restore Certificates**.
21. In the main menu, go to **Local Administration > Interfaces**.
22. Select the relevant interface.



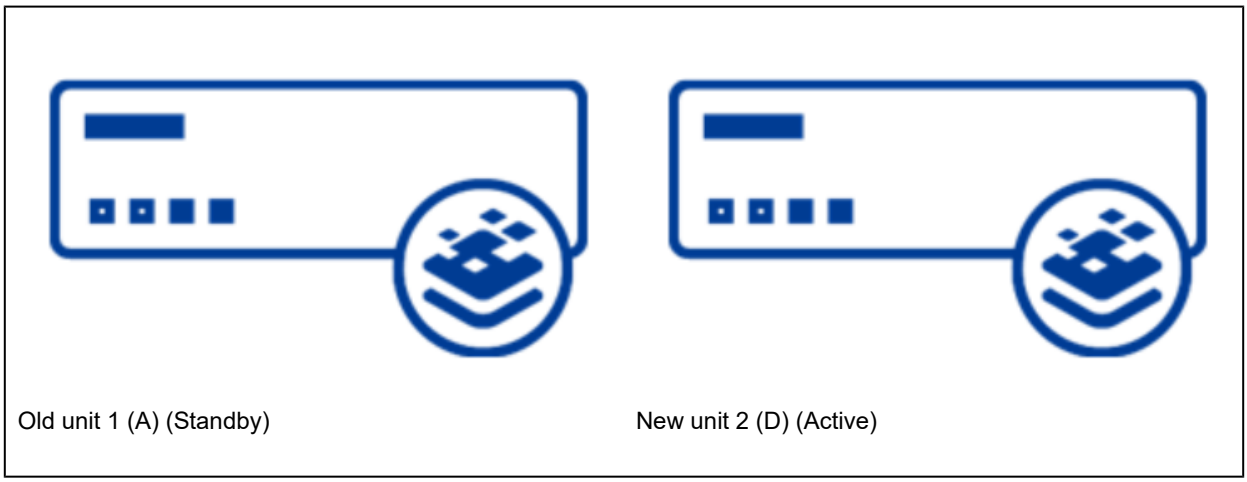
23. Check that the **Interface Address (address[/prefix])**, the **HA Shared IP address** and **HA Partner IP address** are correct before adding it to the production unit.
24. In the main menu, go to **Local Administration > HA Parameters**.



25. Ensure that the **HA Virtual ID** is correct and unique.
26. When the new unit 2 (D) is connected, open the WUI of the shared IP address and in the main menu, go to **System Configuration > HA Parameters**.



27. Click **Force Update**.



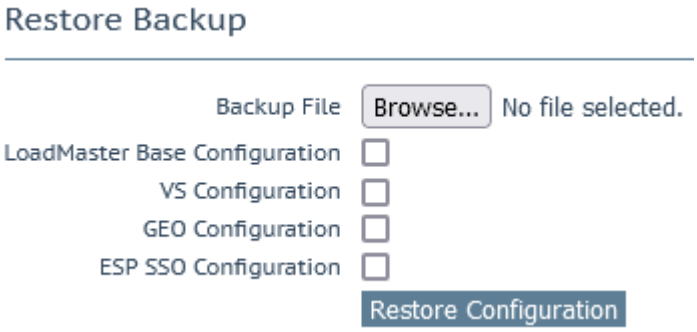
Preferred active: unit 2	
	
New unit 1 (C)	Old unit 2 (B)

Note: This copies the configuration from the old unit 1 (A) (Master) to the new unit 2 (D) (standby). This takes approximately 15 seconds.

28. Now, old unit 1 (A) can be removed from production.

Note: As new unit 2 (D) is active, this should not affect production.

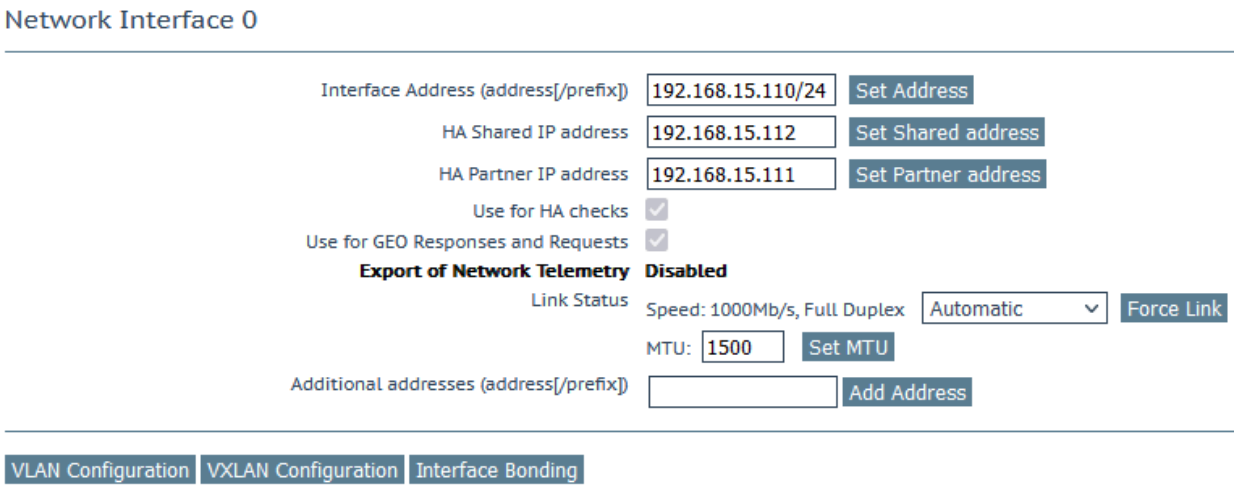
29. On the WUI of the new unit 1 (C), in the main menu, go to **System Configuration > System Administration > Backup/Restore**.



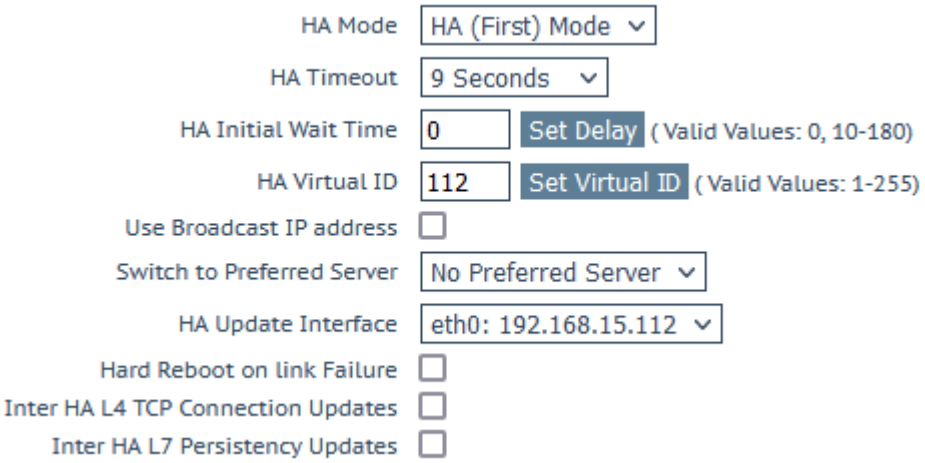
30. Click **Choose File**.
31. Browse to and select the backup file.
32. Select the configuration(s) to be restored.

Note: This is the backup configuration from old unit 1 (A).

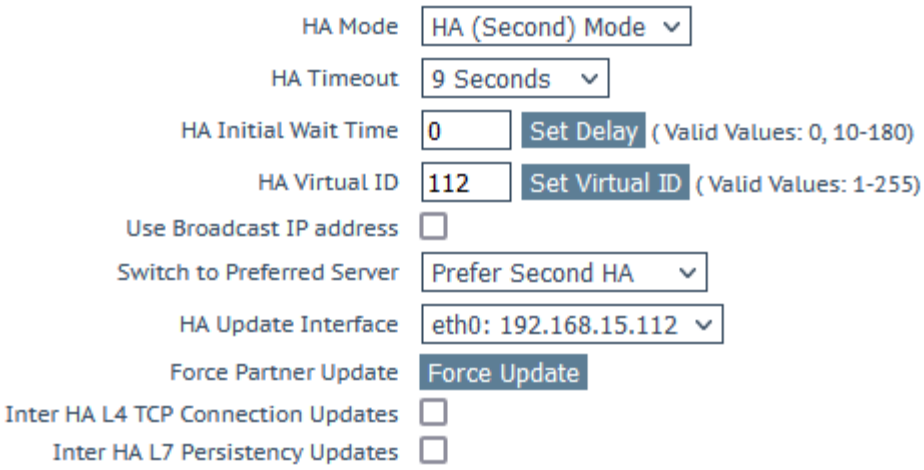
33. Click **Restore Configuration**.
34. Click **Reboot Now**.
35. Click **Continue**.
36. In the main menu, go to **Local Administration > Interfaces**.
37. Select the relevant interface.



38. Check that the **Interface Address (address[/prefix])**, the **HA Shared IP address** and **HA Partner IP address** are correct before adding it to the production unit.
39. In the main menu, go to **Local Administration > HA Parameters**.



40. Ensure that the **HA Virtual ID** is correct and unique.
41. When new unit 1 (C) is connected, open the WUI of the shared IP address and in the main menu, go to **System Configuration > HA Parameters**.



42. Click **Force Update**.

43. This takes approximately 15 seconds.



New unit 1 (C) (Standby)

Preferred active set to none

Current setup – two units in production



New unit 2 (D) (Active)



Old unit 1 (A)



Old unit 2 (B)

Ensure the **Partner Shared Secret** matches in both the active and standby unit. You can find this secret in the following locations:

- Regular/shared WUI: **Certificates & Security > Remote Access**
- Local WUI (of a configured HA unit): **Local Administration > Remote Access**

12

References

Unless otherwise specified, the following documents can be found at https://docs.progress.com/.

LoadMaster HA for Azure, Installation Guide

LoadMaster HA for AWS, Installation Guide

Web User Interface (WUI), Configuration Guide

Feature Description, LoadMaster Clustering