

# Appliance Quick Start Guide

Version 8.9.1 Revision 1.0.0



# Table of Contents

1. About this Guide .....	3
2. Appliance Configuration Overview .....	3
3. Appliance Security .....	3
Security Mode .....	3
Passwords .....	4
The 'loadbalancer' WebUI account .....	4
The 'root' Linux account .....	4
4. Deployment Concept .....	4
5. One-Arm and Two-Arm Topologies .....	5
6. Supported Load Balancing Methods .....	6
7. Ports Used by the Appliance .....	7
8. Appliance Deployment .....	7
Virtual Appliance .....	8
Hardware Appliance .....	8
Cloud Appliances .....	8
AWS .....	8
Azure .....	8
Google Cloud Platform .....	8
9. Configuring Initial Network Settings .....	8
10. Accessing the Appliance WebUI .....	14
Main Menu Options .....	15
11. Installing the License Key .....	16
12. Appliance Software Update .....	17
Determining the Current Software Version .....	17
Checking for Updates using Online Update .....	17
Using Offline Update .....	17
13. Configuring & Testing a Simple Load Balanced Test Environment .....	18
STEP 1 - Deploy the Appliance .....	19
STEP 2 - Run the Network Setup Wizard .....	19
STEP 3 - Configure the Virtual Service (VIP) & Associated Real Servers (RIPs) .....	19
Virtual Service Configuration .....	19
Real Server Configuration .....	20
STEP 4 - Finalizing the Configuration .....	20
STEP 5 - Viewing & Modifying the Configuration .....	20
STEP 6 - Checking the Status using System Overview .....	21
STEP 7 - Verification & Testing .....	22
14. Configuring HA - Adding a Secondary Appliance .....	24
Non-Replicated Settings .....	24
Adding a Secondary Appliance - Create an HA Clustered Pair .....	25
15. More Information .....	26
16. Loadbalancer.org Technical Support .....	26
Contacting Support .....	27

# 1. About this Guide

This quick start guide provides enough information to deploy the appliance, configure a simple load balanced test environment and test and verify its functionality.

## Note

Please also refer to the [Administration Manual](#) for much more detailed information on setting up the appliance and configuring a load balancing solution. For information on configuring the appliance for specific applications, please refer to our extensive library of [Deployment Guides](#).

## 2. Appliance Configuration Overview

Initial network configuration is carried out at the console using the Network Setup Wizard. Once the wizard has been run, load balanced services can be configured using the WebUI; either using the Setup Wizard (for Layer 7 services) or by manually defining the Virtual Services (VIPs) and associated Real Servers (RIPs).

By default, the WebUI is accessible on HTTPS port **9443**, this can be changed if required. For more information please refer to the "Appliance Security" section below.

We always recommend that where possible two appliances are deployed as a clustered pair for high availability and resilience, this avoids introducing a single point of failure to your network.

We recommend that the Primary appliance is fully configured first, then the Secondary appliance can be added to create an HA pair. Once the HA pair is configured, load balanced services are automatically synchronized from the Primary to Secondary appliance. Load balanced services should then be configured & modified on the Primary appliance and the Secondary will be automatically kept in sync. For more information on configuring an HA pair, please refer to [Configuring HA - Adding a Secondary Appliance](#).

## 3. Appliance Security

## Note

For full details of all security related features, please refer to [Appliance Security Features](#).

### Security Mode

To control how the appliance is accessed and which features are enabled, 3 security modes are provided:

- **Custom** - In this mode the security options can be configured to suit your requirements
- **Secure - (default)** - In this mode:
  - The WebUI is accessible on HTTPS port **9443**, if you attempt to access the WebUI on HTTP port **9080** you will be redirected to HTTPS port **9443**
  - Access to the *Local Configuration > Execute shell command* menu option is disabled
  - The ability to edit the firewall script & the firewall lockdown wizard script is disabled
  - 'root' user console & SSH password access are disabled
- **Secure - Permanent** - This mode is the same as **Secure** but once set it cannot be changed



 **Important** Only set the security mode to **Secure - Permanent** if you are 100% sure this is what you want!

To configure the Security Mode:

1. Using the WebUI, navigate to: **Local Configuration > Security**.
2. Select the required **Appliance Security Mode** - if **Custom** is selected, configure the additional options according to your requirements.
3. Click **Update**.

## Passwords

The password for the '**root**' user Linux account and the '**loadbalancer**' WebUI user account are set during the Network Setup Wizard. These can be changed at any time.

### Note

The passwords for the cloud products are either set to a default value or are configured during instance deployment. Also, for Enterprise AWS and Enterprise Azure it's not possible to directly log in as root. For more details, please refer to the relevant [Quick Start Configuration Guide](#).

### The 'loadbalancer' WebUI account

This can be changed using the WebUI menu option: **Maintenance > Passwords**.

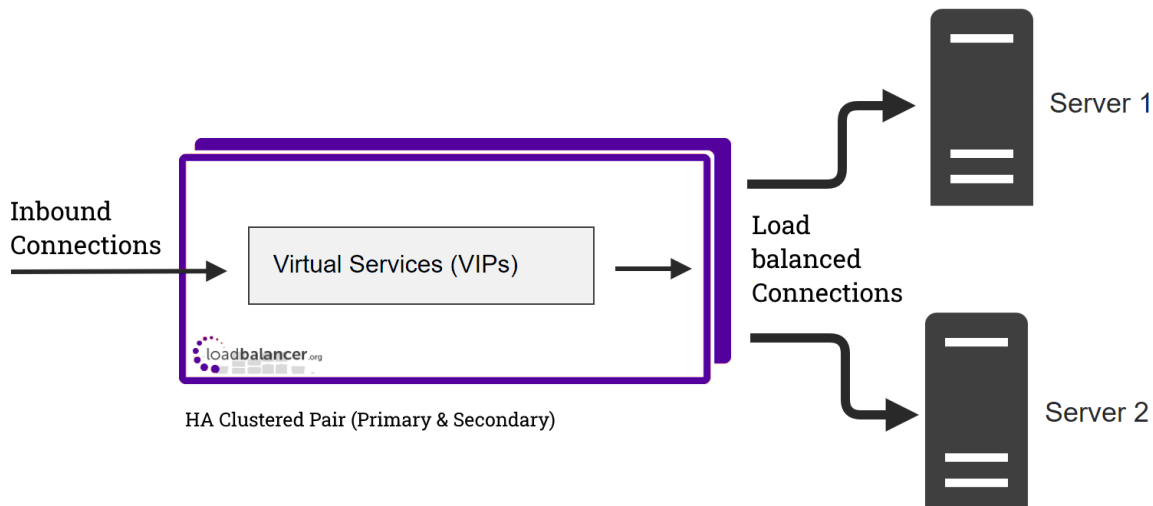
### The 'root' Linux account

As explained in [Security Mode](#) above, 'root' user console & SSH password access are disabled by default. Once enabled, the 'root' password can be changed at the console, or via an SSH session using the following command:

```
# passwd
```

## 4. Deployment Concept

Once deployed, clients connect to the Virtual Service(s) (VIPs) on the load balancer rather than connecting directly to one of the load balanced servers. Requests are then distributed between the load balanced servers according to the load balancing algorithm selected.



#### Note

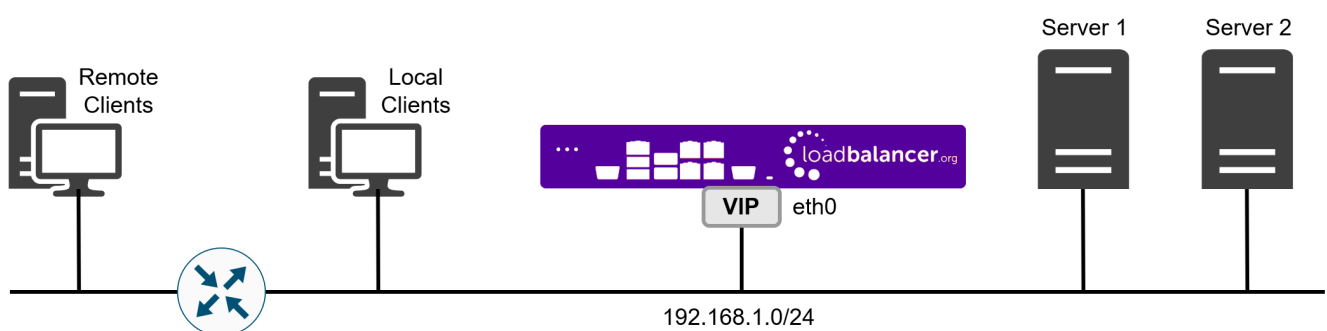
We always recommend that 2 appliances are deployed as an active/passive HA pair. The Secondary appliance automatically takes over if the Primary unit fails. For more information on configuring HA using 2 appliances please refer to [Configuring HA - Adding a Secondary Appliance](#).

## 5. One-Arm and Two-Arm Topologies

The number of 'arms' is a descriptive term for how many interfaces are used to connect a device to a network. It's common for a load balancer that uses a routing method (NAT) to have a two-arm configuration although one-arm is also supported. Proxy based load balancers (SNAT) commonly use a one-arm configuration although two-arm is also supported.

### One-Arm

The VIP and the load balanced servers are located in a single subnet. The load balancer requires a single network interface adapter - **eth0** in the diagram below.



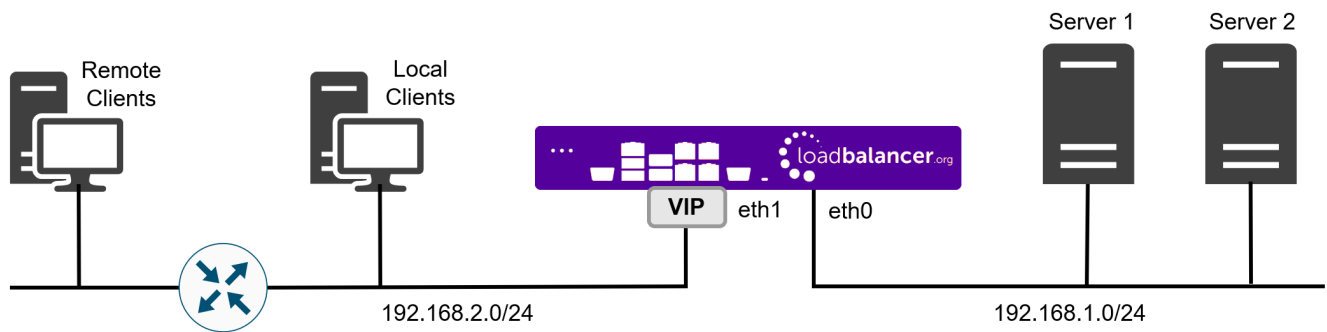
### Two-Arm

Here, 2 subnets are used. The VIP is located in one subnet and the load balanced Real Servers are located in the other. The load balancer requires 2 interfaces, one in each subnet as shown in the diagram below.

#### Note

This can be achieved by using two network adapters, or by creating VLANs on a single adapter.





### Note

Typically **eth0** is used as the internal interface and **eth1** is used as the external interface. This is not a requirement - each interface can be used for any purpose.

## 6. Supported Load Balancing Methods

The Loadbalancer.org appliance is one of the most flexible load balancers available. The design allows different load balancing modules to utilize the core high availability framework of the appliance. Multiple load balancing methods can be used at the same time or in combination with each other. The table below describes the methods supported by the appliance.

Layer	Method	Comments	Topology	Note
Layer 4	DR (Direct Routing)	Ultra-fast local server based load balancing <ul style="list-style-type: none"> <li>Requires the "ARP problem" to be solved on each Real Server - for more details please refer to <a href="#">DR Mode Considerations</a></li> </ul>	One-Arm (*)	1
Layer 4	NAT (Network Address Translation)	Fast Layer 4 load balancing <ul style="list-style-type: none"> <li>The appliance must be the default gateway for the Real Servers</li> </ul>	One or Two-Arm	1
Layer 4	TUN	Similar to DR but works across IP encapsulated tunnels	One-Arm	2
Layer 4	SNAT (Source Network Address Translation)	Fast layer 4 SNAT supporting both TCP & UDP <ul style="list-style-type: none"> <li>Very simple to implement</li> <li>Requires no Real Server configuration changes</li> </ul>	One or Two-Arm	3
Layer 7	SSL Termination (STunnel, Pound & HAProxy)	Usually required in order to process cookie persistence in HTTPS streams on the load balancer <ul style="list-style-type: none"> <li>SSL Termination is processor intensive</li> </ul>	One or Two-Arm	4



Layer	Method	Comments	Topology	Note
Layer 7	SNAT (Source Network Address Translation using HAProxy)	Layer 7 allows greater flexibility including full SNAT and remote server load balancing, cookie insertion and URL switching <ul style="list-style-type: none"> <li>• Very simple to implement</li> <li>• Requires no Real Server configuration changes</li> <li>• Not as fast as Layer 4 methods</li> </ul>	One or Two-Arm	4

(\*) DR mode can also be used in a multi-homed configuration where real servers are located in different subnets. In this case, the load balancer must have an interface in the same subnet to enable layer 2 connectivity which is required for DR mode to operate.

### Notes

1. Recommended for high performance fully transparent and scalable solutions.
2. Only required for Direct Routing implementation across routed networks (rarely used).
3. Recommended when you want to load balance both TCP and UDP but you're unable to use DR mode or NAT mode due to network topology or Real Server related reasons.
4. Recommended if HTTP cookie persistence is required, also used for several Microsoft applications such as Exchange, SharePoint & Remote Desktop Services and for overall deployment simplicity since Real Servers can be on any accessible subnet and no Real Server changes are required.

## 7. Ports Used by the Appliance

By default, the appliance uses the following TCP & UDP ports:

Protocol	Port	Purpose
TCP	22	SSH
TCP & UDP	53	DNS
TCP & UDP	123	NTP
TCP & UDP	161	SNMP
UDP	6694	Heartbeat between Primary & Secondary appliances in HA mode
TCP	7778	HAProxy persistence table replication
TCP	9080	WebUI - HTTP (disabled by default)
TCP	9081	Nginx fallback page
TCP	9443	WebUI - HTTPS

## 8. Appliance Deployment



## Virtual Appliance

A fully featured, fully supported 30 day trial is available if you are conducting a PoC (Proof of Concept) deployment. The VA is currently available for VMware, Virtual Box, Hyper-V, KVM, XEN and Nutanix AHV and has been optimized for each Hypervisor. By default, the VA is allocated 2 vCPUs, 4GB of RAM and has a 20GB virtual disk. The Virtual Appliance can be downloaded [here](#).

### Note

The same download is used for the licensed product, the only difference is that a license key file (supplied by our sales team when the product is purchased) must be applied using the appliance's WebUI.

### Note

Please refer to [Virtual Appliance Installation](#) and the ReadMe.txt text file included in the VA download for additional information on deploying the VA using the various Hypervisors.

### Note

The VA has 4 network adapters. For VMware only the first adapter (**eth0**) is connected by default. For HyperV, KVM, XEN and Nutanix AHV all adapters are disconnected by default. Use the network configuration screen within the Hypervisor to connect the required adapters.

## Hardware Appliance

For details of installing and connecting the appliance, please refer to [Hardware Appliance Installation](#).

## Cloud Appliances

### AWS

For details of deploying and configuring the Amazon Web Services (AWS) appliance please refer to the [AWS Configuration Guide](#).

### Azure

For details of deploying and configuring the Microsoft Azure appliance please refer to the [Azure Configuration Guide](#).

### Google Cloud Platform

For details of deploying and configuring the Google Cloud appliance please refer to the [GCP Configuration Guide](#).

## 9. Configuring Initial Network Settings

After power up, the following startup message is displayed on the appliance console:





```

Welcome to the Loadbalancer.org appliance.

To perform initial network configuration, log in to the console as
Username: setup
Password: setup

To access the web interface and wizard, point your browser at
http://192.168.2.21:9080/
or
https://192.168.2.21:9443/

lbmaster login:

```

As mentioned in the text, to perform initial network configuration, login as the 'setup' user at the appliance console.

Once logged in, the Network Setup Wizard will start automatically. This will enable you to configure the management IP address and other network settings for the appliance.

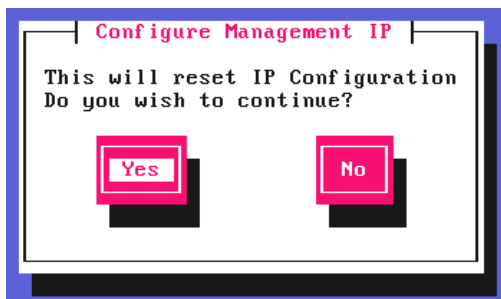
login to the console:

**Username:** setup

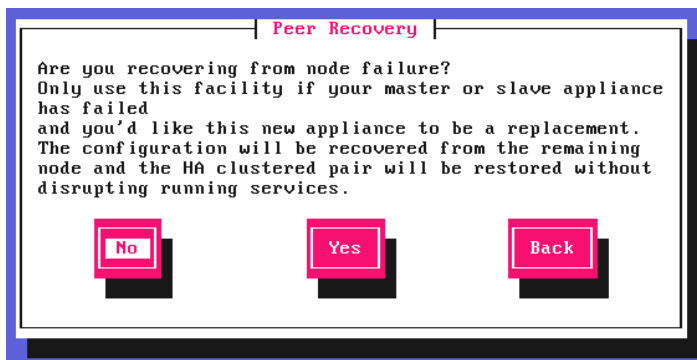
**Password:** setup

A series of screens will be displayed that allow network settings to be configured:

In the **Configure Management IP** screen, leave **Yes** selected and hit <ENTER> to continue.



In the **Peer Recovery** screen, leave **No** selected and hit <ENTER> to continue.



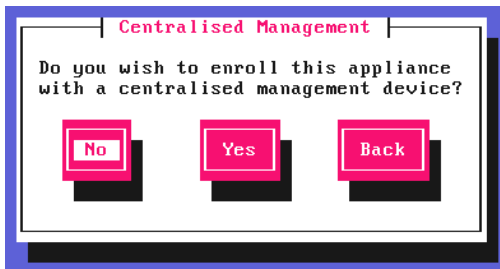
#### Note

For more details on node recovery using this option please refer to [Disaster Recovery After Node](#)



(Primary or Secondary) Failure.

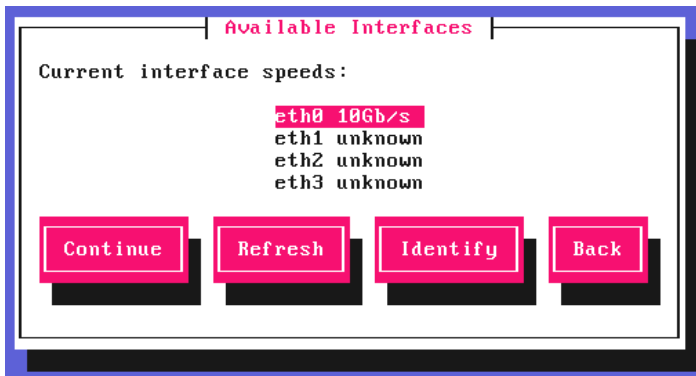
In the **Centralized Management** screen, if you have been provided with Management Server details select **Yes**, otherwise leave **No** selected, then hit <ENTER> to continue.



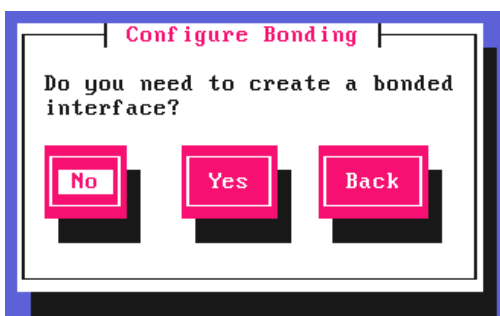
**Note**

For information on how to modify Centralized Management settings via the WebUI, please refer to [Portal Management](#).

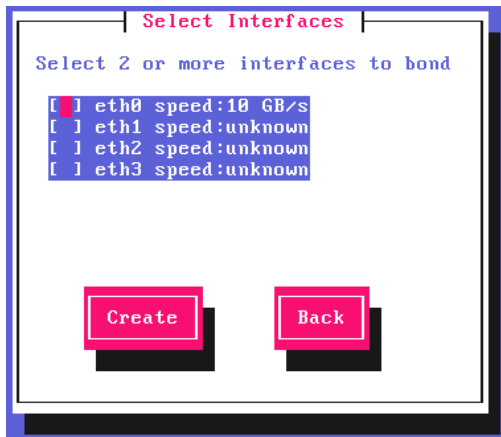
In the **Available Interfaces** screen, a list of available interfaces will be displayed, hit <ENTER> to continue.



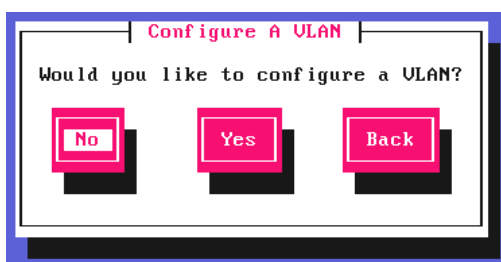
In the **Configure Bonding** screen, select **Yes** if you want to configure a bonded interface, if not leave **No** selected, then hit <ENTER> to continue.



If you select **Yes**, the **Select Interfaces** screen will be displayed. Using the space bar, select the interfaces you'd like to include in the bond, select **Create** and hit <ENTER> to continue.

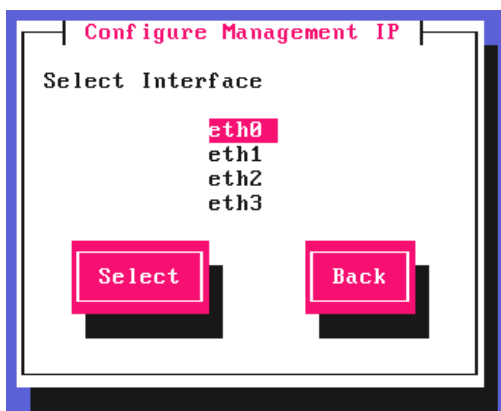


In the **Configure a VLAN** screen, select **Yes** if you want to configure a VLAN, if not leave **No** selected, then hit <ENTER> to continue.



If you select **Yes** you'll be prompted to enter a VLAN Tag ID.

In the **Configure Management IP** screen, select the interface that'll be used to manage the appliance, then hit <ENTER> to continue.



In the **Set IP address** screen, either enter the required *Static IP Address & CIDR Prefix* and select **Done** or select **Use DHCP**, then hit <ENTER> to continue.

**Set IP Address for eth0**

Please enter IP and CIDR Subnet Mask

Static IP Address (eg. 192.168.1.100): 192.168.111.150  
 CIDR Prefix (eg. 24): 18

Done Use DHCP Back

**Note**

A subnet mask such as 255.255.255.0 is not valid, in this case enter 24 instead.

In the **Configure Default Gateway** screen, enter the required *Default Gateway IP Address*, select **Done** and hit <ENTER> to continue.

**Configure Default Gateway**

Please enter IP Address

Default Gateway IP Address (eg. 192.168.1.100): 192.168.64.1

Done Back

In the **Configure DNS Servers** screen, configure the required DNS server(s), select **Done** and hit <ENTER> to continue.

**Configure DNS Servers**

Please enter IP Address

Primary DNS Server (eg. 192.168.1.100): 8.8.8.8  
 Secondary DNS Server (Leave blank to omit):

Done Back

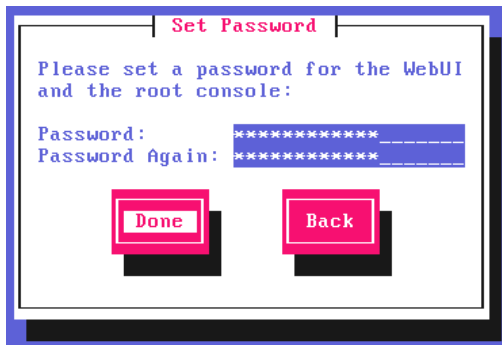
In the **Set Password** screen, hit <ENTER> to continue.

**Set Password**

Please set a password. This password will be used for the WUI and the root console. NOTE: You will not be able to access the console until it is enabled from the WUI.

OK

Enter the *Password* you'd like to use for the 'loadbalancer' WebUI user account and the 'root' Linux user account. Repeat the password, select **Done** and hit <ENTER> to continue.



**Set Password**

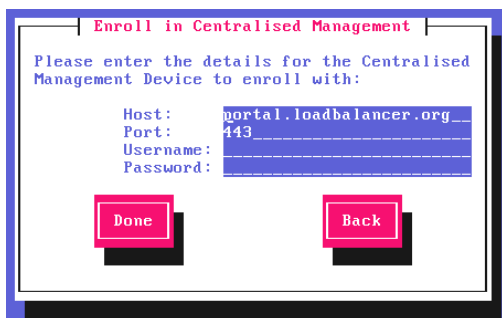
Please set a password for the WebUI and the root console:

Password: \*\*\*\*\*

Password Again: \*\*\*\*\*

**Done** **Back**

If you selected **Yes** when asked if you want to enroll for Centralized Management, you'll now be prompted for the details. Default values for the **Host** and **Port** are set and can be changed if required. Enter a suitable **Username** and **Password**, select **Done** and hit <ENTER> to continue.



**Enroll in Centralised Management**

Please enter the details for the Centralised Management Device to enroll with:

Host: portal.loadbalancer.org

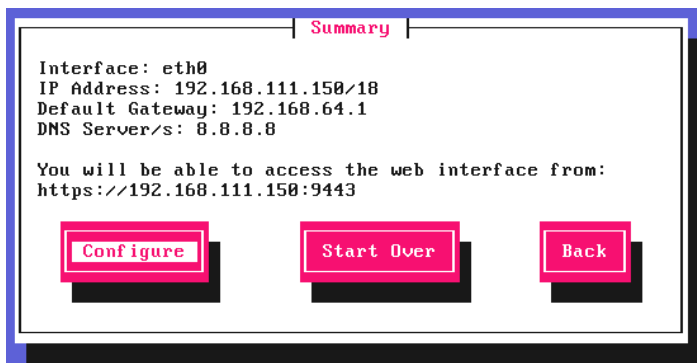
Port: 443

Username: \_\_\_\_\_

Password: \_\_\_\_\_

**Done** **Back**

In the **Summary** screen, check all settings. If everything is correct, leave **Configure** selected and hit <ENTER> to continue. All settings will be applied. If you need to change a setting, use the **Back** button.



**Summary**

Interface: eth0

IP Address: 192.168.111.150/18

Default Gateway: 192.168.64.1

DNS Server/s: 8.8.8.8

You will be able to access the web interface from:  
https://192.168.111.150:9443

**Configure** **Start Over** **Back**

Once the configuration has been written, the **Configuration Complete** screen and message will be displayed. Click **OK** to exit the wizard and return to the command prompt.



**Configuration complete**

The configuration has been written successfully.

**OK**

## 10. Accessing the Appliance WebUI

The WebUI is accessed using a web browser. By default, users are authenticated using Apache authentication. Users can also be authenticated against LDAP, LDAPS, Active Directory or Radius - for more information, please refer to [External Authentication](#).

### Note

There are certain differences when accessing the WebUI for the cloud appliances. For details, please refer to the relevant [Quick Start / Configuration Guide](#).

### Note

A number of compatibility issues have been found with various versions of Microsoft Internet Explorer and Edge. The WebUI has been tested and verified using both Chrome & Firefox.

1. Using a browser, navigate to the following URL:

**<https://<IP-address-configured-during-the-network-setup-wizard>:9443/lbadmin/>**

### Note

You'll receive a warning about the WebUI's certificate. This is due to the default self signed certificate that is used. If preferred, you can upload your own certificate - for more information, please refer to [Appliance Security Features](#).

2. Log in to the WebUI using the following credentials:

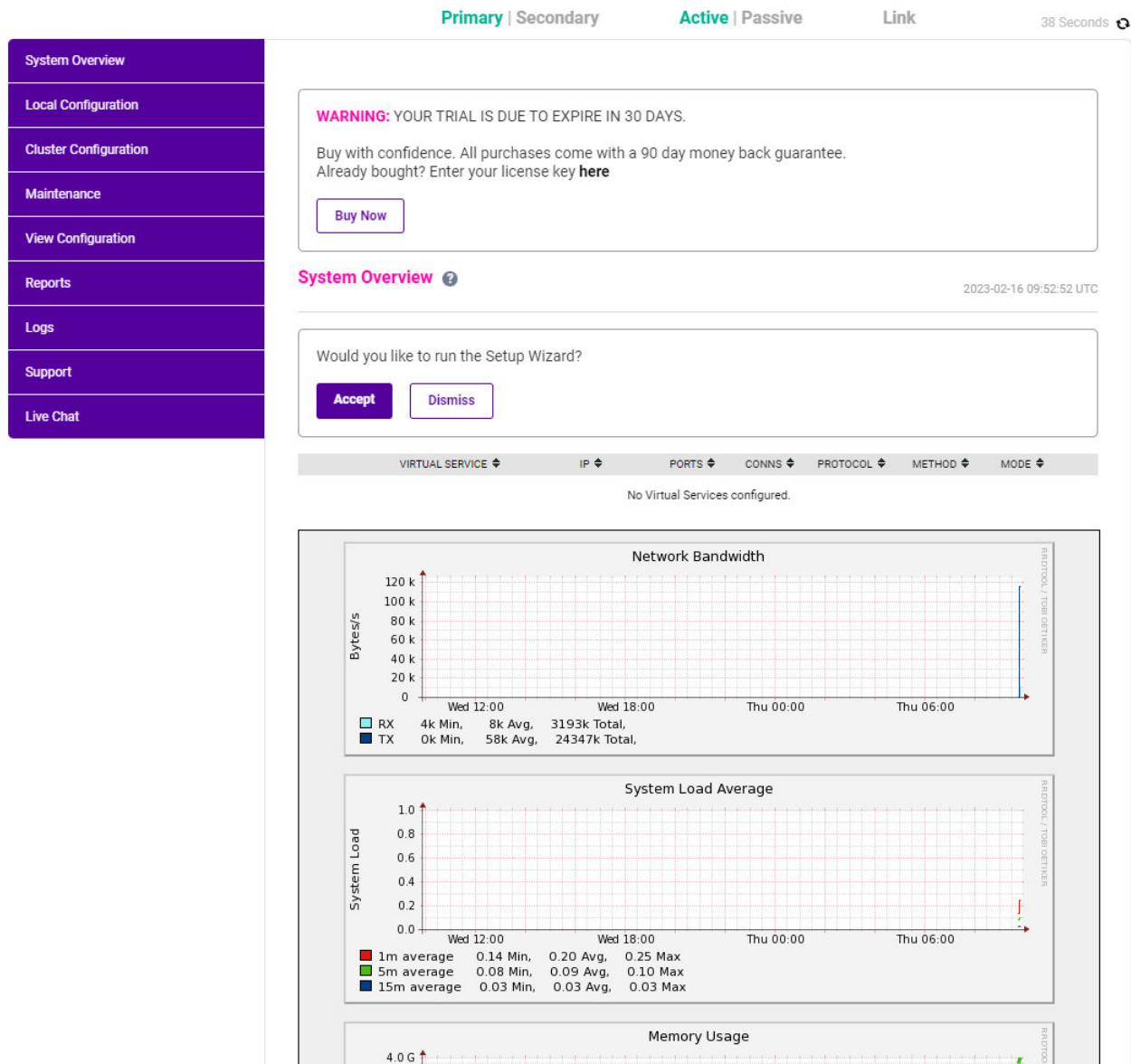
**Username:** loadbalancer

**Password:** <configured-during-network-setup-wizard>

### Note

To change the password, use the WebUI menu option: ***Maintenance > Passwords***.

Once logged in, the WebUI will be displayed as shown below:



3. You'll be asked if you want to run the Setup Wizard. Click **Dismiss** if you're following a guide or want to configure the appliance manually. Click **Accept** to start the Setup Wizard.



#### Note

The Setup Wizard can only be used to configure Layer 7 services.

## Main Menu Options

**System Overview** - Displays a graphical summary of all VIPs, RIPs and key appliance statistics

**Local Configuration** - Configure local host settings such as IP address, DNS, system time etc.

**Cluster Configuration** - Configure load balanced services such as VIPs & RIPs

**Maintenance** - Perform maintenance tasks such as service restarts and taking backups

**View Configuration** - Display the saved appliance configuration settings

**Reports** - View various appliance reports & graphs

**Logs** - View various appliance logs

**Support** - Create a support download, contact the support team & access useful links

## 11. Installing the License Key

The appliance can be used completely unrestricted for 30 days without installing a license key. After 30 days, the appliance continues to work but it's no longer possible to make configuration changes.

### Note

if you're conducting a PoC (Proof of Concept) using the VA and require more time to complete your evaluation, please contact [sales@loadbalancer.org](mailto:sales@loadbalancer.org) who will be able to provide guidance on how to extend the trial.

For an unlicensed VA, the following message is displayed:

**WARNING:** YOUR TRIAL IS DUE TO EXPIRE IN 30 DAYS.

Buy with confidence. All purchases come with a 90 day money back guarantee.  
Already bought? Enter your license key **here**

**Buy Now**

For an unlicensed hardware appliance, the following message is displayed:

**WARNING:** This appliance is unregistered. **Please enter your license key** within 30 days to activate your appliance.  
If you do not have your license key please **Contact Us**

*To install the license key:*

1. Using the WebUI, navigate to: *Local Configuration > License Key*.

### Install License Key

This unit is in evaluation mode. Please enter your license key to remove this restriction.

If you do not have a license key, please contact [sales@loadbalancer.org](mailto:sales@loadbalancer.org).

No file chosen

**Install License Key**

2. Click **Choose File** then browse to and select the license file provided when the appliance was purchased.
3. Click **Install License Key**.

### Note

Once the license is applied, these warning messages will no longer be displayed.



## 12. Appliance Software Update

To ensure that the appliance(s) are running the latest software version, we recommend a software update check is performed.

### Determining the Current Software Version

The software version is displayed at the bottom of the WebUI as shown in the example below:

Copyright © Loadbalancer.org Inc. 2002 – 2023  
ENTERPRISE VA Max - v8.9.0

English ▼

### Checking for Updates using Online Update

#### Note

By default, the appliance periodically contacts the Loadbalancer.org update server and checks for updates. An update check can also be manually triggered as detailed below.

1. Using the WebUI, navigate to: **Maintenance > Software Update**.
2. Select **Online Update**.
3. If the latest version is already installed, a message similar to the following will be displayed:

**Information:** Version v8.9.0 is the current release. No updates are available

4. If an update is available, you'll be presented with a list of new features, improvements, bug fixes and security related updates.
5. Click **Online Update** to start the update process.

#### Note

Do not navigate away whilst the update is ongoing, this may cause the update to fail.

6. Once complete (the update can take several minutes depending on download speed and upgrade version) the following message will be displayed:

**Information:** Update completed successfully.

7. If services need to be reloaded/restarted or the appliance needs a full restart, you'll be prompted accordingly.

### Using Offline Update

If the load balancer does not have access to the Internet, offline update can be used.





## Note

Please contact [support@loadbalancer.org](mailto:support@loadbalancer.org) to check if an update is available and obtain the latest offline update files.

To perform an offline update:

1. Using the WebUI, navigate to: **Maintenance > Software Update**.
2. Select **Offline Update**.
3. The following screen will be displayed:

## Software Update

### Offline Update

The following steps will lead you through offline update.

1. Contact **Loadbalancer.org support** to obtain the offline update archive and checksum.
2. Save the archive and checksum to your local machine.
3. Select the archive and checksum files in the upload form below.
4. Click **Upload and Install** to begin the update process.

Archive:  No file chosen

Checksum:  No file chosen

4. Select the **Archive** and **Checksum** files.
5. Click **Upload and Install**.
6. If services need to be reloaded/restarted or the appliance needs a full restart, you'll be prompted accordingly.

## 13. Configuring & Testing a Simple Load Balanced Test Environment

This configuration example illustrates how to configure a simple layer 7 load balanced test environment.



## Note

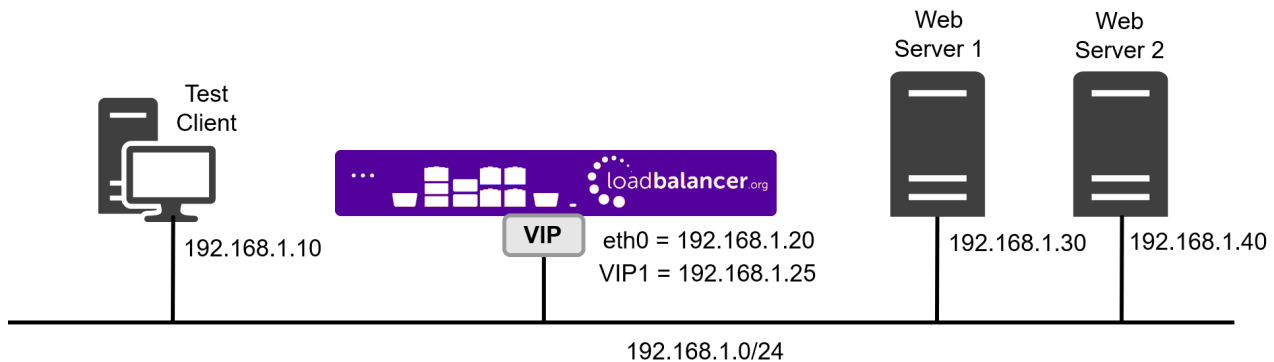
Layer 7 SNAT mode is used in the example. As mentioned earlier, this is not the fastest mode but is very simple to deploy and requires no mode specific configuration changes to the Real Servers.

The following table & diagram describe the environment:

IP Address	Device	Notes
192.168.1.10	Test Client	
192.168.1.20	Load Balancer	the load balancer's own IP address
192.168.1.25	Load Balancer	the Virtual IP address (VIP), the IP address clients connect to



IP Address	Device	Notes
192.168.1.30	Web Server 1	the first Real Server (RIP)
192.168.1.40	Web Server 2	the second Real Server (RIP)



## STEP 1 - Deploy the Appliance

Please refer to [Appliance Deployment](#).

## STEP 2 - Run the Network Setup Wizard

Please refer to [Configuring Initial Network Settings](#).

## STEP 3 - Configure the Virtual Service (VIP) & Associated Real Servers (RIPs)

### Virtual Service Configuration

1. Using the WebUI, navigate to *Cluster Configuration > Layer 7 – Virtual Services* and click **Add a new Virtual Service**.
2. Enter the following details:

Virtual Service		[Advanced +]
Label	<input type="text" value="web-Cluster"/>	?
IP Address	<input type="text" value="192.168.1.25"/>	?
Ports	<input type="text" value="80"/>	?
<b>Protocol</b>		
Layer 7 Protocol	<input type="text" value="HTTP Mode"/>	?
		<input type="button" value="Cancel"/> <input type="button" value="Update"/>

- Specify an appropriate *Label* (name) for the Virtual Service, e.g. **Web-Cluster**.
- Set the *IP Address* field to the required address, e.g. **192.168.1.25**.

- Set the *Ports* field to the required port, e.g. **80**.
- Leave the *Protocol* set to **HTTP Mode**.

3. Click **Update** to create the Virtual Service.

## Real Server Configuration

1. Using the WebUI, navigate to: *Cluster Configuration > Layer 7 – Real Servers* and click **Add a new Real Server** next to the newly created VIP.
2. Enter the following details:

Label	<input type="text" value="Web1"/>	?
Real Server IP Address	<input type="text" value="192.168.1.30"/>	?
Real Server Port	<input type="text" value="80"/>	?
Re-Encrypt to Backend	<input type="checkbox"/>	?
Enable Redirect	<input type="checkbox"/>	?
Weight	<input type="text" value="100"/>	?

Cancel
Update

- Specify an appropriate *Label* for the RIP, e.g. **Web1**.
- Set the *Real Server IP Address* field to the required address, e.g. **192.168.1.30**.
- Set the *Real Server Port* field to the required port, e.g. **80**.

3. Click **Update** to add the Real Server.

4. Now repeat these steps to add the second Real Server, e.g. **Web2**.

### Note

By default, Real Server health-checks are set to use a TCP port connect. If you need a more robust check, this can be changed by modifying the configuration as explained below. For more information, please refer to [Real Server Health Monitoring & Control](#).

## STEP 4 - Finalizing the Configuration

To apply the new settings, HAProxy must be reloaded. This can be done using the button in the "Commit changes" box at the top of the screen or by using the **Restart Services** menu option:

1. Using the WebUI, navigate to: *Maintenance > Restart Services*.
2. Click **Reload HAProxy**.

## STEP 5 - Viewing & Modifying the Configuration

1. The VIP can be viewed using the WebUI menu option: *Cluster Configuration > Layer 7 - Virtual Services* as shown below:



## Layer 7 - Virtual Services

Search..

Add a new Virtual Service

Service Name	IP	Port	Config Type		
Web-Cluster	192.168.1.25	Ports 80	Auto	Modify	Delete

- Clicking the **Modify** button allows all VIP settings to be modified.
  - If changes are made, click the **Update** button to save the changes, then use the **Reload HAProxy** button in the "Commit changes" box at the top of the screen to apply the changes.
2. The RIP(s) can be viewed using the WebUI menu option: *Cluster Configuration > Layer 7 - Real Services* as shown below:



## Layer 7 - Real Servers

Web-Cluster	192.168.1.25	Ports 80	Add a new Real Server		
Web1	192.168.1.30	80	Weight 100	Modify	Delete
Web2	192.168.1.40	80	Weight 100	Modify	Delete

- Clicking the **Modify** button allows all RIP settings to be modified.
- If changes are made, click the **Update** button to save the changes, then use the **Reload HAProxy** button in the "Commit changes" box at the top of the screen to apply the changes.

## STEP 6 - Checking the Status using System Overview

1. Using the WebUI, navigate to: *System Overview* to view the newly created VIP & RIPs. Green indicates that the associated RIPs are passing their health checks:

System Overview ?							2023-01-31 14:16:55 UTC
VIRTUAL SERVICE	IP	PORTS	CONNS	PROTOCOL	METHOD	MODE	
 Web-Cluster	192.168.1.25	80	0	HTTP	Layer 7	Proxy	

2. Click anywhere on the VIP's horizontal grey area to expand the VIP and view the RIPs:

	VIRTUAL SERVICE	IP	PORTS	CONNS	PROTOCOL	METHOD	MODE	
↑	Web-Cluster	192.168.1.25	80	0	HTTP	Layer 7	Proxy	
	REAL SERVER	IP	PORTS	WEIGHT	CONNS			
↑	Web1	192.168.1.30	80	100	0	Drain	Halt	
↑	Web2	192.168.1.40	80	100	0	Drain	Halt	

## STEP 7 - Verification & Testing

1. Verify that both Real Servers are up. In the example below, Web2 is failing its health-check:

	VIRTUAL SERVICE	IP	PORTS	CONNS	PROTOCOL	METHOD	MODE	
⚠	Web-Cluster	192.168.1.25	80	0	HTTP	Layer 7	Proxy	
	REAL SERVER	IP	PORTS	WEIGHT	CONNS			
↑	Web1	192.168.1.30	80	100	0	Drain	Halt	
↓	Web2	192.168.1.40	80	100	0	Drain	Halt	

- This should be investigated and corrected - possible steps include:
  - Verify that the application/service is running on the Real Server.
  - Make sure you can ping the Real Server from the load balancer - either from the console, via an SSH session or using the WebUI menu option: *Local Configuration > Execute Shell Command*.

To enable shell commands to be run from the WebUI, the appliance Security Mode must be set to **Custom**:

### Note

1. Using the WebUI, navigate to: *Local Configuration > Security*.
2. Set *Appliance Security Mode* to **Custom**.
3. Click **Update**.

If you run ping from the WebUI, use the form:

### Note

```
ping -c 4 192.168.1.40
```

The **-c 4** means ping 4 times then stop.

- Verify that the application/service is up and available when accessed from the load balancer - various methods can be used:

- Using **telnet** at the console or via an SSH session:

```
telnet 192.168.1.40 80
```

The following shows a successful connection to port 80:

```
Trying 192.168.1.40...
Connected to 192.168.1.40.
Escape character is '^['.
```

- Using **nmap** at the console, via an SSH session or using the WebUI option: *Local Configuration > Execute Shell Command*:

```
nmap 192.168.1.40
```

The following is displayed for a working server:

```
Starting Nmap 5.51 ( http://nmap.org ) at 2022-10-25 14:18 UTC
Nmap scan report for 192.168.1.40
Host is up (0.00056s latency).
Not shown: 995 filtered ports
PORT      STATE SERVICE
80/tcp    open  http
135/tcp   open  msrpc
443/tcp   open  https
445/tcp   open  microsoft-ds
3389/tcp  open  ms-term-serv
MAC Address: 00:50:56:82:0B:D3 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 4.87 seconds
```

This shows that the server is listening on port 80.

- Using **curl** at the console, via an SSH session or using the WebUI option: *Local Configuration > Execute Shell Command*:

```
curl http://192.168.1.40
or
curl http://host.mydomain.com
```

For a working web server listening on port 80, the default page is returned.

2. Once both servers are up (shown green) browse to the VIP address and verify that you see the web page from each Real Server:

- Halt Web1 using the **Halt** option for Web1 in the System Overview and verify that content is served by Web2 on a browser refresh.

- Bring Web1 back online using the **Online (Halt)** option for Web1, then halt Web2 and verify that content is served by Web1 on a browser refresh.

#### Note

For more configuration examples using Layer 7 SNAT mode as well as other modes, please refer to [Configuration Examples](#).

#### Note

For additional guidance on diagnosing and resolving any issues you may have, please also refer to [Diagnostics & Troubleshooting](#).

## 14. Configuring HA - Adding a Secondary Appliance

Our recommended configuration is to use a clustered HA pair of load balancers to provide a highly available and resilient load balancing solution.

We recommend that the Primary appliance is configured first and then the Secondary should be added. Once the Primary and Secondary are paired, all load balanced services configured on the Primary are automatically replicated to the Secondary over the network using SSH/SCP.

The clustered HA pair uses Heartbeat to determine the state of the other appliance. Should the active device (normally the Primary) suffer a failure, the passive device (normally the Secondary) will take over.

### Non-Replicated Settings

A number of settings are not replicated as part of the Primary/Secondary pairing process and therefore must be manually configured on the Secondary appliance. These are listed by WebUI menu option in the table below:

WebUI Main Menu Option	Sub Menu Option	Description
Local Configuration	Hostname & DNS	Hostname and DNS settings
Local Configuration	Network Interface Configuration	All network settings including IP address(es), bonding configuration and VLANs
Local Configuration	Routing	Routing configuration including default gateways and static routes
Local Configuration	System Date & time	All time and date related settings
Local Configuration	Physical – Advanced Configuration	Various settings including Internet Proxy, Management Gateway, Firewall connection tracking table size, NIC offloading, SMTP relay, logging and Syslog Server
Local Configuration	Security	Appliance security settings
Local Configuration	SNMP Configuration	Appliance SNMP settings
Local Configuration	Graphing	Appliance graphing settings
Local Configuration	License Key	Appliance licensing
Maintenance	Software Updates	Appliance software update management
Maintenance	Firewall Script	Appliance firewall (iptables) configuration





WebUI Main Menu Option	Sub Menu Option	Description
Maintenance	Firewall Lockdown Wizard	Appliance management lockdown settings

### ⚠ Important

Make sure that if these settings/updates have been configured on the Primary appliance, they're also configured on the Secondary appliance.


## Adding a Secondary Appliance - Create an HA Clustered Pair

### 📌 Note

If you have already run the firewall lockdown wizard on either appliance, you'll need to ensure that it is temporarily disabled on both appliances whilst performing the pairing process.

1. Deploy a second appliance that will be the Secondary and configure initial network settings.
2. Using the WebUI on the Primary appliance, navigate to: **Cluster Configuration > High-Availability Configuration**.

### Create a Clustered Pair

 **LOADBALANCER**

**Local IP address**

192.168.110.40

**IP address of new peer**

192.168.110.41


**Password for *loadbalancer* user on peer**

••••••••••

**Add new node**


3. Specify the IP address and the **loadbalancer** user's password for the Secondary (peer) appliance as shown in the example above.
4. Click **Add new node**.
5. The pairing process now commences as shown below:


## Create a Clustered Pair

 **LOADBALANCER**

Primary

IP: 192.168.110.40

  
Attempting to pair..

 **LOADBALANCER**

Secondary

IP: 192.168.110.41

Local IP address

192.168.110.40

IP address of new peer

192.168.110.41


Password for *loadbalancer* user on peer

••••••••••

configuring


6. Once complete, the following will be displayed on the Primary appliance:

## High Availability Configuration - primary

 **LOADBALANCER**

Primary

IP: 192.168.110.40

 **LOADBALANCER**

Secondary

IP: 192.168.110.41

Break Clustered Pair

Make Active

7. To finalize the configuration, restart heartbeat and any other services as prompted in the "Commit changes" message box at the top of the screen.

### Note

Clicking the **Restart Heartbeat** button on the Primary appliance will also automatically restart heartbeat on the Secondary appliance.

### Note

For more details on configuring HA with 2 appliances, please refer to [Appliance Clustering for HA](#).

### Note

For details on testing and verifying HA, please refer to [Clustered Pair Diagnostics](#).

## 15. More Information

Please refer to our website for all the latest [Manuals](#) and [Deployment Guides](#).

## 16. Loadbalancer.org Technical Support

Our highly experienced Support Engineers are on hand to help 24 hours a day, 365 days a year.



## Contacting Support

If you have any questions regarding the appliance or need assistance with load balancing your application, please don't hesitate to contact [support@loadbalancer.org](mailto:support@loadbalancer.org).





**Visit us:** [www.loadbalancer.org](http://www.loadbalancer.org)

**Phone us:** +44 (0)330 380 1064

**Phone us:** +1 833 274 2566

**Email us:** [info@loadbalancer.org](mailto:info@loadbalancer.org)

**Follow us:** [@loadbalancer.org](https://twitter.com/loadbalancer.org)

## About Loadbalancer.org

Loadbalancer.org's mission is to ensure that its clients' businesses are never interrupted. The load balancer experts ask the right questions to get to the heart of what matters, bringing a depth of understanding to each deployment. Experience enables Loadbalancer.org engineers to design less complex, unbreakable solutions - and to provide exceptional personalized support.

