LOADBALANCER

DEPLOYMENT GUIDE

Load Balancing Philips Healthcare Vue PACS

Version 1.0

Table of Contents

1. About this Guide

This guide details the steps required to configure a load balanced Philips Healthcare Vue PACS environment utilizing Loadbalancer.org appliances. It covers the configuration of the load balancers and also any Vue PACS configuration changes that are required to enable load balancing.

1.1. Acronyms & Terminology Used in the Guide

Acronym	Description
WFM	Work Flow Manager
EIS	Extensible Integration Software (Worklist Server)
VIP	Virtual IP address - the IP address of the load balanced cluster of RIPs, the address presented to connecting clients. Also refers to the logical load balancer configuration and is used as an acronym for Virtual Service.
RIP	The Real IP address - the IP address of a backend server in the cluster. Also refers to the logical load balancer configuration and is used as an acronym for Real Server.
Virtual Service	The main building block used to define load balanced services. It defines the IP address clients connect to, which Real Servers are load balanced and other settings such as health check options, persistence options and timeout settings.
Real Server	The actual backend server being load balanced. Multiple Real Servers are associated with a Virtual Service.

2. Prerequisites

1. Ensure that firewalls and other network devices are configured to allow management and other required access to the appliance - for details of all ports used refer to Ports Used by the Appliance.
2. Ensure that firewalls and other network devices are configured to allow client/test access to all Virtual Services (VIPs).
3. Ensure that firewalls and other network devices are configured to allow load balancer access to all Vue PACS servers.
4. Have IP addresses for the appliance and all required Virtual Services.

3. Software Versions Supported

3.1. Loadbalancer.org Appliance

- V8.8.1 & later

3.2. Philips Vue PACS

- V12.2.5 & later

4. Load Balancing Philips Vue PACS

ℹ Note	It's highly recommended that you have a working Vue PACS environment first before implementing the load balancer.

4.1. Virtual Services (VIP) Requirements

To provide load balancing and HA for Vue PACS, the following VIPs are required:

Ref.	VIP Name	Mode/Type	Port(s)	Persistence	Health Check
VIP 1	DICOM_VIP	L7 SNAT	2104	Source IP	Connect to Port
VIP 2	DMWL_VIP	L7 SNAT	3320	Source IP	Connect to Port
VIP 3	PORTAL_VIP	L7 SNAT	80	Source IP	External Script
VIP 3-B1	CHAT	L7 SNAT	-	None	HTTPS (GET)
VIP 4	PORTAL_VIP_STANDBY	L7 SNAT	80	Source IP	External Script
VIP 4-B1	CHAT_STANDBY	L7 SNAT	-	None	HTTPS (GET)
VIP 5	CLIENT_VIP	L7 SNAT	80,443,514,2104,22104,32338	Source IP	Connect to Port
VIP 6	CLIENT_DB_VIP	L7 SNAT	1521	Source IP	Connect to Port
VIP 7	HL7_VIP	L7 SNAT	10010,4001,4003,4005	Source IP	Connect to Port

ℹ Note	VIPs with references in the format **VIP <number>-B<number>** are ***Backend Only*** VIPs. These define a pool of Real Servers and are used for chat and syscfg traffic. ACL's are used by the 'parent' VIP to determine when the ***Backend Only*** VIPs are used based on the requested URL.

ℹ Note	VIP 4 - PORTAL_VIP_STANDBY is only required when there is a secondary site and that site has multiple Portal servers. If the standby site has a single server VIP 4 is not needed.

(!) Important	Ensure that the required DNS records are created that point to the appropriate VIP. If DNS records already exist, ensure that they are modified to point to the VIP rather than individual servers.

4.2. SSL Termination

SSL Termination is configured on the load balancer for the following VIPs:

- VIP 3 - PORTAL_VIP
- VIP 4 - PORTAL_VIP_STANDBY

This provides a corresponding HTTPS Virtual Service for each VIP. Certificates in PEM or PFX format can be uploaded or if required a CSR can be generated on the load balancer to request a new certificate.

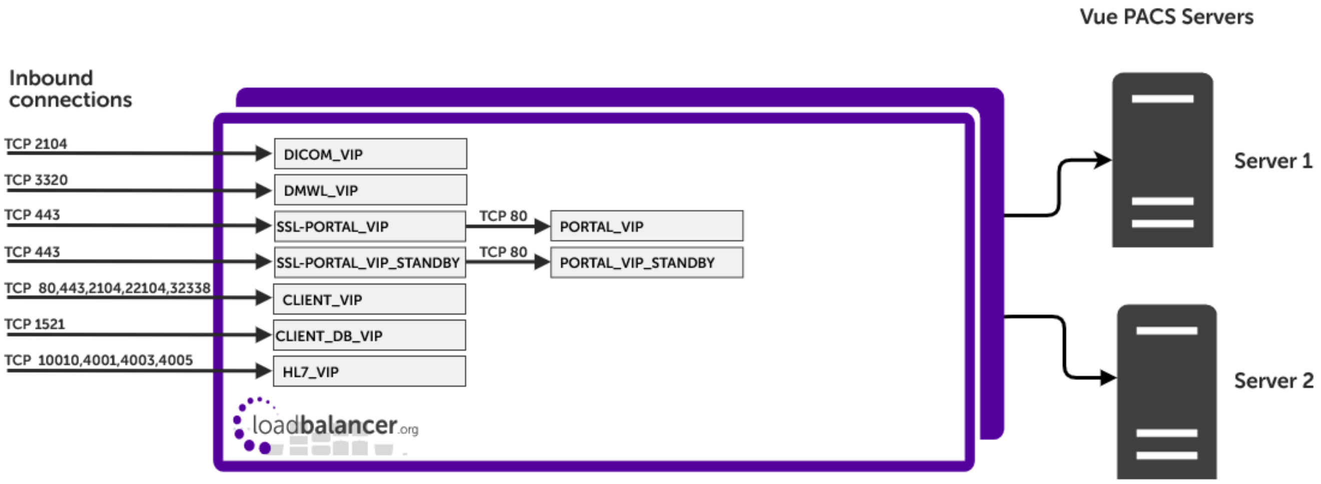
5. Ports Used by the Appliance

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

Protocol	Port	Purpose
TCP	22 *	SSH
TCP & UDP	53 *	DNS / GSLB
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	9000 *	Gateway service (Centralized/Portal Management)
TCP	9080 *	WebUI - HTTP (disabled by default)
TCP	9081 *	Nginx fallback page
TCP	9443 *	WebUI - HTTPS
TCP	25565 *	Shuttle service (Centralized/Portal Management)

Note The ports used for SSH, GSLB, SNMP, the WebUI, the fallback page, the gateway service and the shuttle service can be changed if required. For more information, please refer to Service Socket Addresses.

6. Deployment Concept



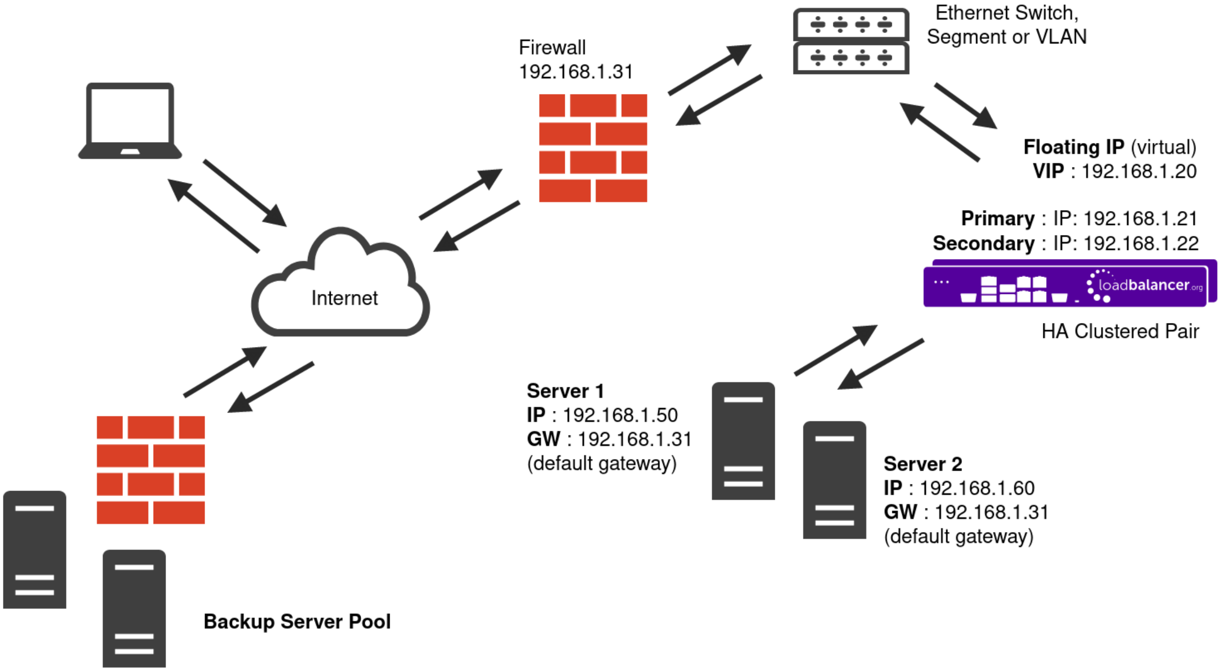
VIP = **V**irtual **IP** Address

7. Load Balancer Deployment Methods

For Vue PACS, both layer 4 DR mode and layer 7 SNAT mode are used. These modes are described below and are used for the configurations presented in this guide.

7.1. Layer 7 SNAT Mode

Layer 7 SNAT mode uses a proxy (HAProxy) at the application layer. Inbound requests are terminated on the load balancer and HAProxy generates a new corresponding request to the chosen Real Server. As a result, Layer 7 is typically not as fast as the Layer 4 methods. Layer 7 is typically chosen when either enhanced options such as SSL termination, cookie based persistence, URL rewriting, header insertion/deletion etc. are required, or when the network topology prohibits the use of the layer 4 methods.



- Because layer 7 SNAT mode is a full proxy, any server in the cluster can be on any accessible subnet including across the Internet or WAN.
- Layer 7 SNAT mode is not transparent by default, i.e. the Real Servers will not see the source IP address of the client, they will see the load balancer's own IP address by default, or any other local appliance IP address if preferred (e.g. the VIP address). This can be configured per layer 7 VIP. If required, the load balancer can be configured to provide the actual client IP address to the Real Servers in 2 ways. Either by inserting a header that contains the client's source IP address, or by modifying the Source Address field of the IP packets and replacing the IP address of the load balancer with the IP address of the client. For more information on these methods please refer to Transparency at Layer 7.
- Layer 7 SNAT mode can be deployed using either a one-arm or two-arm configuration. For two-arm deployments, **eth0** is normally used for the internal network and **eth1** is used for the external network although this is not mandatory.
- Requires no mode-specific configuration changes to the load balanced Real Servers.
- Port translation is possible with Layer 7 SNAT mode, e.g. VIP:80 → RIP:8080 is supported.

- You should not use the same RIP:PORT combination for layer 7 SNAT mode VIPs and layer 4 SNAT mode VIPs because the required firewall rules conflict.

8. Configuring Vue PACS for Load Balancing

8.1. Layer 7 SNAT Mode

Layer 7 SNAT mode VIPs do not require any mode specific configuration changes to the load balanced Real Servers (Vue PACS Servers).

9. Load Balancer Appliance Installation & Configuration for Vue PACS

9.1. Overview

For Vue PACS deployments, 2 load balancer appliances must be installed and configured and then paired to create an active/passive HA clustered pair.

The following is an overview of the installation and configuration process:

1. Deploy 2 hardware appliances - refer to Section 9.2
2. Configure the management IP address and other basic settings on **both** appliances - refer to Section 9.3
3. Run a software update check on **both** appliances - refer to Section 9.6
4. Configure the appliance security mode on **both** appliances - refer to Section 9.7
5. Verify network connections and configure any additional settings on **both** appliances - refer to Section 9.8
6. Configure the required load balanced services on the **Primary** appliance - refer to Section 9.9
7. Restart services on the **Primary** appliance - refer to Section 9.9.10
8. Verify that everything is working as expected on the **Primary** appliance - refer to Section 11
9. Configure the HA Pair on the **Primary** appliance - this will replicate all load balanced services to the Secondary appliance, once configured the Secondary appliance will be kept in-sync automatically - refer to Section 12
10. Configure any required optional settings on **both** appliances - refer to Section 13

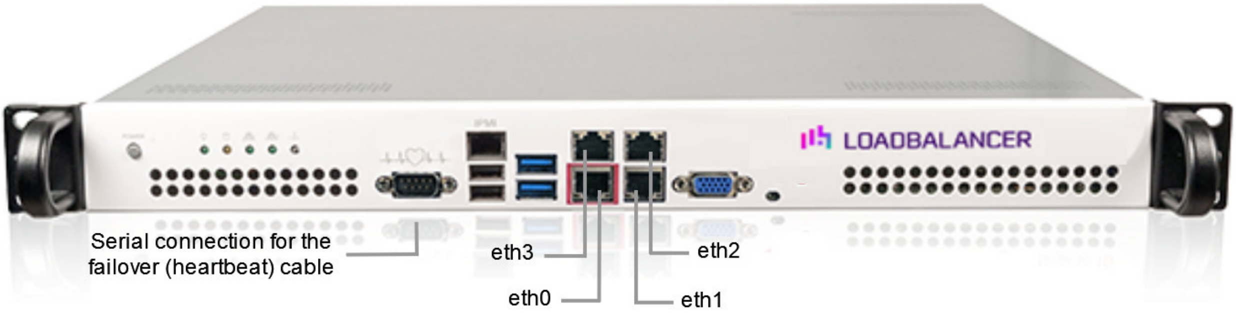
9.2. Hardware Appliance Installation

Follow the steps below to install 2 appliances, one as the Primary the other as the Secondary.

1. Remove all packaging and rack mount the appliance if required.
2. Connect the power lead.

> **Note** The power supply is an auto-sensing unit (100v to 240v).

3. Connect network cables from all 4 interfaces (eth0 to eth3) to the relevant switch. All interfaces are configured as a single bond in the following section (Section 9.3).
4. Attach a monitor & keyboard to the appliance.



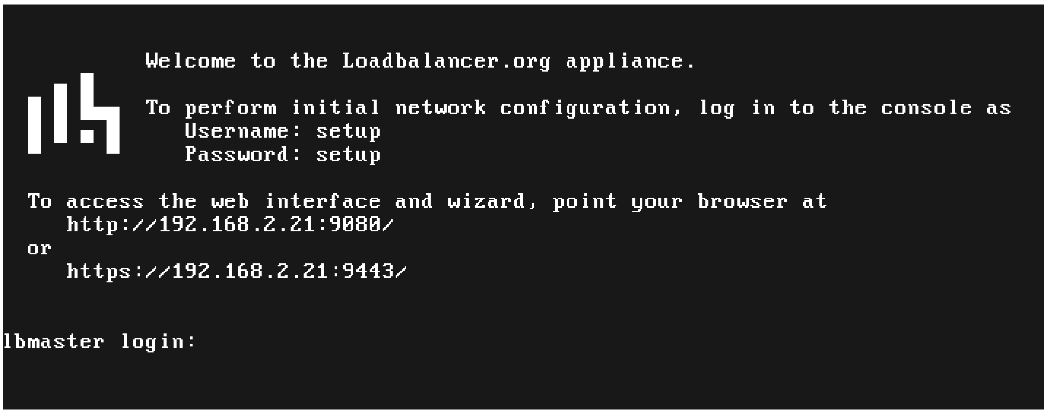
> **Note** The above image shows the Enterprise Prime. For network interface information for other models please refer to Front & Rear Panel Layouts.

Once both appliances are installed, connect a serial (heartbeat) cable between them.

Check that mains power is on and power up both appliances. The fans should start & the front panel LEDs should light.

9.3. 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.

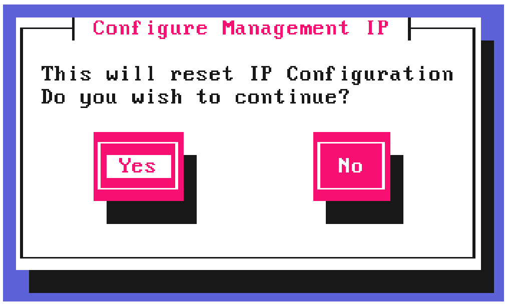
Once logged in, the Network Setup Wizard will start automatically. This will enable you to configure the management IP address and other network settings for the appliance.

login to the console:

Username: setup
Password: setup

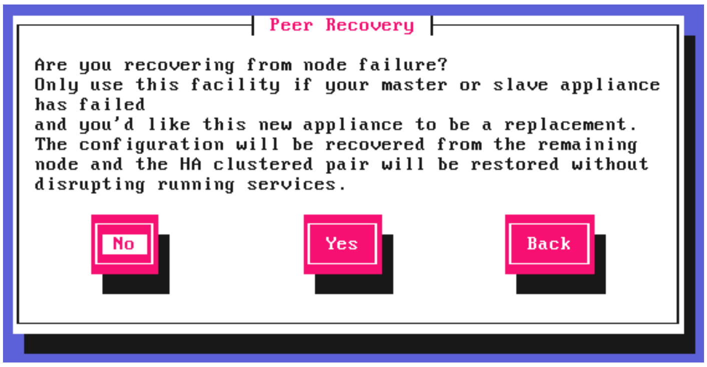
A series of screens will be displayed that allow network settings to be configured:

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



```
Configure Management IP

This will reset IP Configuration
Do you wish to continue?
```

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

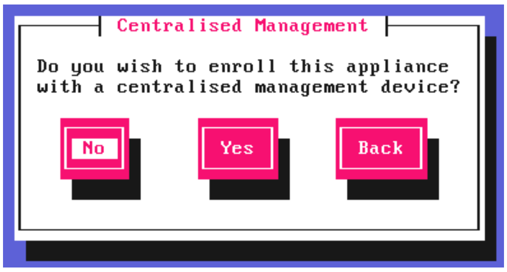


```
Peer Recovery

Are you recovering from node failure?
Only use this facility if your master or slave appliance
has failed
and you'd like this new appliance to be a replacement.
The configuration will be recovered from the remaining
node and the HA clustered pair will be restored without
disrupting running services.
```

ℹ **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.

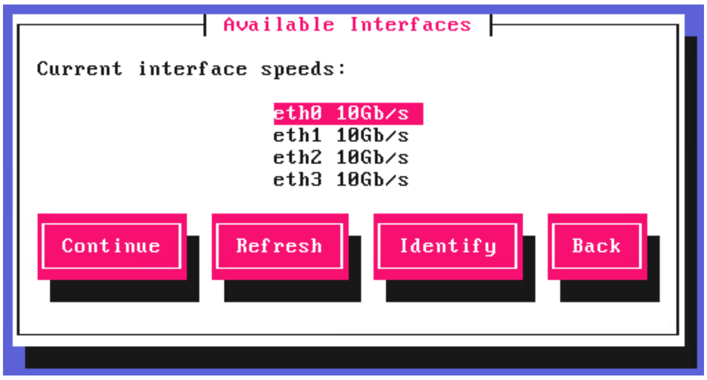


```
Centralised Management

Do you wish to enroll this appliance
with a centralised management device?
```

ℹ **Note**

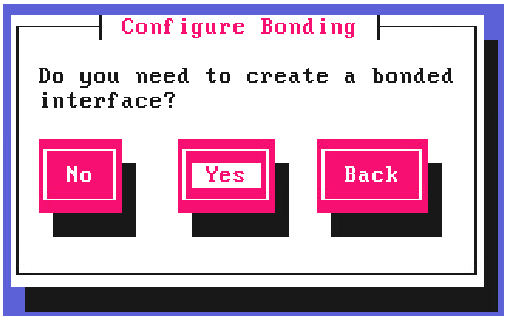
For information on how to modify Centralized Management settings via the WebUI, please refer to Portal Management & Appliance Adoption.

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



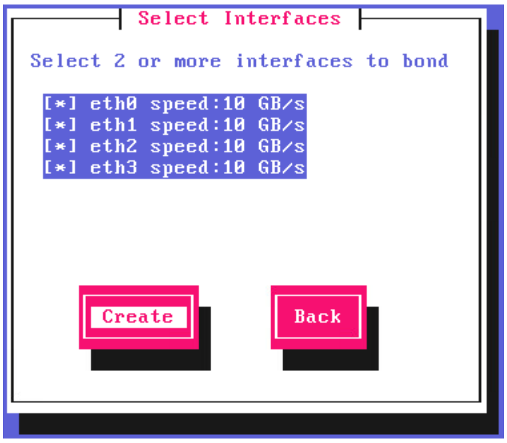
```
Available Interfaces

Current interface speeds:

                    eth0 10Gb/s
                    eth1 10Gb/s
                    eth2 10Gb/s
                    eth3 10Gb/s
```

In the **Configure Bonding** screen, select **Yes** and hit <ENTER> to continue.



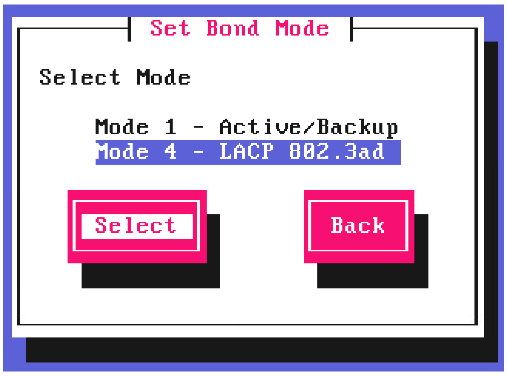
```
Configure Bonding

Do you need to create a bonded
interface?
```

The **Select Interfaces** screen will be displayed. Using the space bar, select all 4 interfaces for the bond, select **Create** and hit <ENTER> to continue.



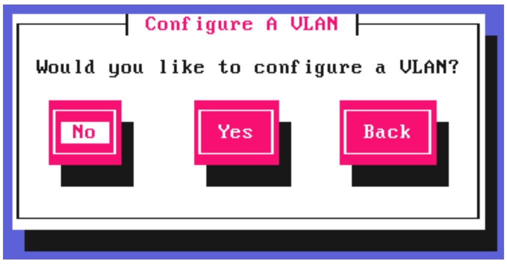
```
Select Interfaces

Select 2 or more interfaces to bond

  [*] eth0 speed:10 GB/s
  [*] eth1 speed:10 GB/s
  [*] eth2 speed:10 GB/s
  [*] eth3 speed:10 GB/s
```

In the **Set Bond Mode** screen, select **Mode 4 - LACP 802.3ad**, select the **Select** button and hit <ENTER> to continue.



```
Set Bond Mode

Select Mode

    Mode 1 - Active/Backup
    Mode 4 - LACP 802.3ad
```

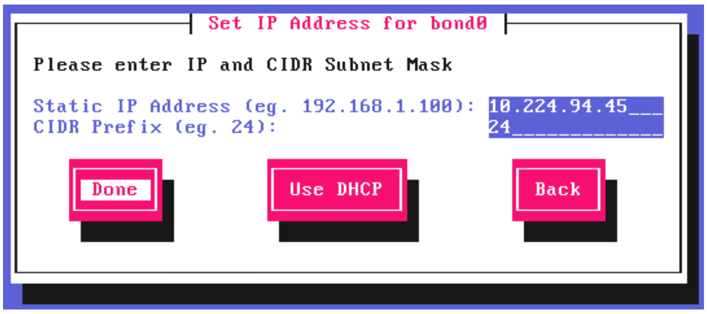
In the **Configure a VLAN** screen, leave **No** selected, then hit <ENTER> to continue.



Configure A VLAN

Would you like to configure a VLAN?

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



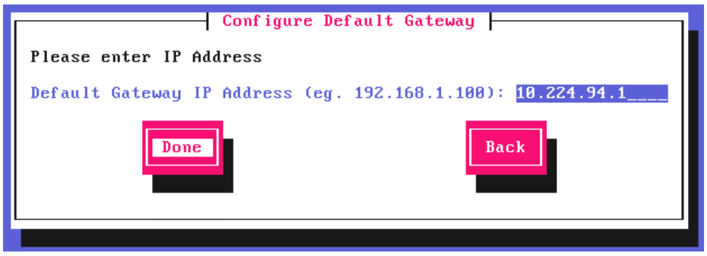
Set IP Address for bond0

Please enter IP and CIDR Subnet Mask

```
Static IP Address (eg. 192.168.1.100): 10.224.94.45___
CIDR Prefix (eg. 24):                  24_____________
```

ℹ 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.

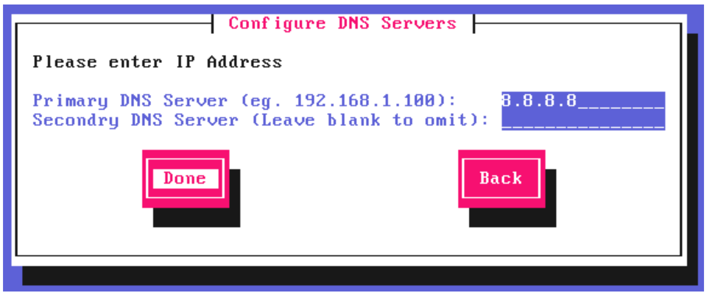


Configure Default Gateway

Please enter IP Address

```
Default Gateway IP Address (eg. 192.168.1.100): 10.224.94.1____
```

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

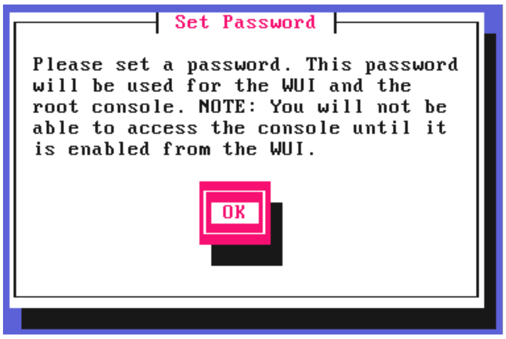


Configure DNS Servers

Please enter IP Address

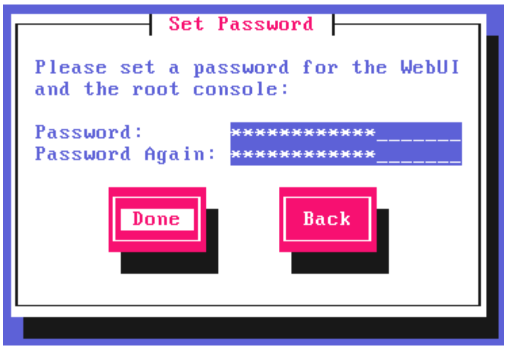
```
Primary DNS Server (eg. 192.168.1.100):    8.8.8.8________
Secondry DNS Server (Leave blank to omit): _______________
```

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



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.

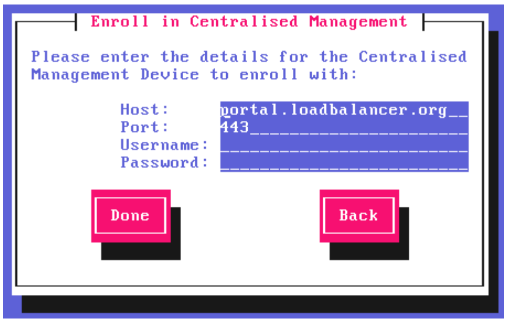
Enter the *Password* you'd like to use for the **loadbalancer** WebUI user account and the **root** Linux user account. Repeat the password, select **Done** and hit <ENTER> to continue.



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

Password: ************_______
Password Again: ************_______

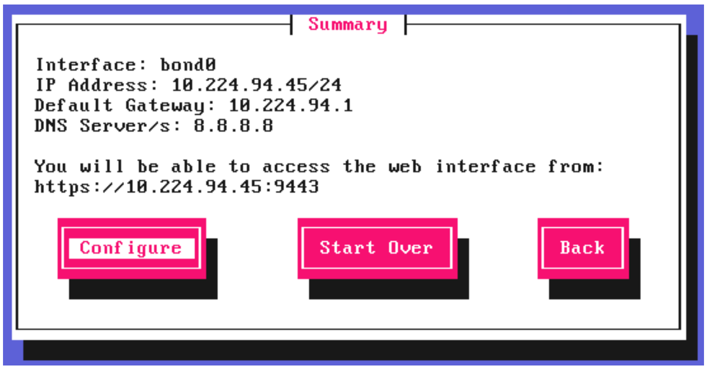
If you selected **Yes** when asked if you want to enroll for Centralized Management, you'll now be prompted for the details. Default values for the *Host* and *Port* are set and can be changed if required. Enter the *Username* and *Password* for the management server account you'd like the appliance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



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

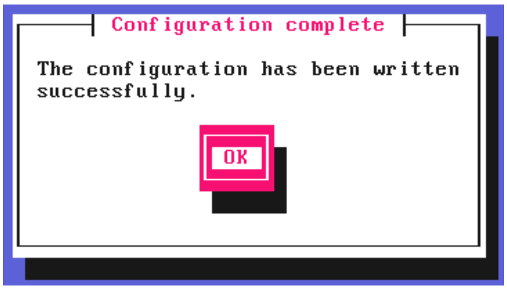
```
Host:      portal.loadbalancer.org__
Port:      443______________________
Username:  _________________________
Password:  _________________________
```

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.



```
Interface: bond0
IP Address: 10.224.94.45/24
Default Gateway: 10.224.94.1
DNS Server/s: 8.8.8.8

You will be able to access the web interface from:
https://10.224.94.45:9443
```

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.

9.4. 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.

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 SSL 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.

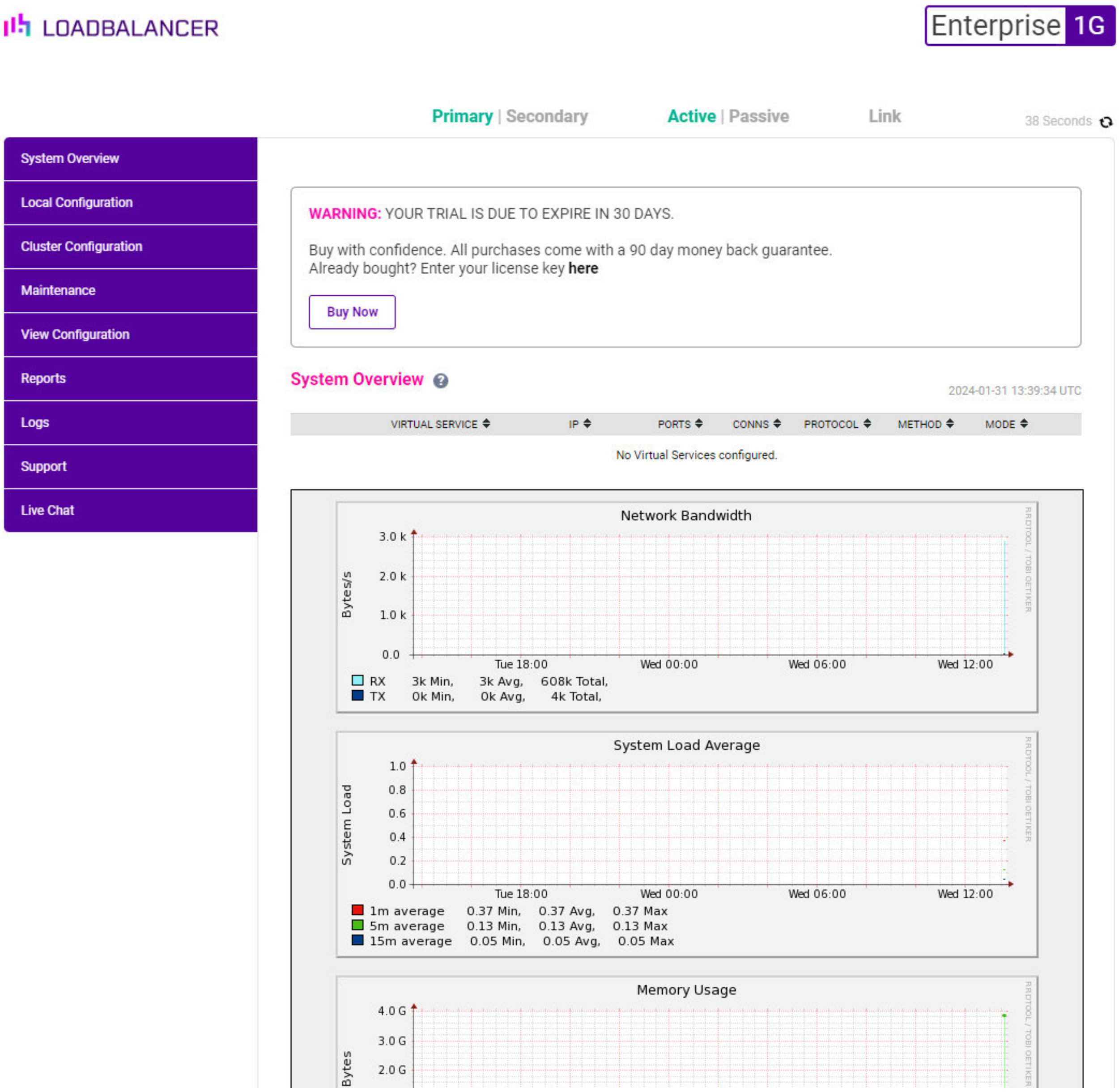
Note	If you need to change the port, IP address or protocol that the WebUI listens on, please refer to Service Socket Addresses.

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:



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**

System Overview

2024-01-31 13:39:34 UTC

VIRTUAL SERVICE ⬍	IP ⬍	PORTS ⬍	CONNS ⬍	PROTOCOL ⬍	METHOD ⬍	MODE ⬍

No Virtual Services configured.

```
RX   3k Min,   3k Avg,   608k Total,
TX   0k Min,   0k Avg,     4k Total,
```

```
1m average    0.37 Min,   0.37 Avg,   0.37 Max
5m average    0.13 Min,   0.13 Avg,   0.13 Max
15m average    0.05 Min,   0.05 Avg,   0.05 Max
```

9.4.1. 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

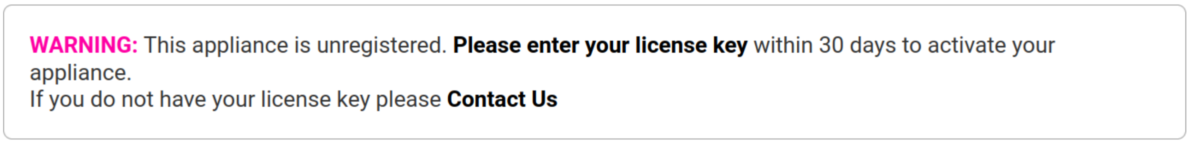
Support - Create a support download, contact the support team & access useful links

Live Chat - Start a live chat session with one of our Support Engineers

9.5. 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.

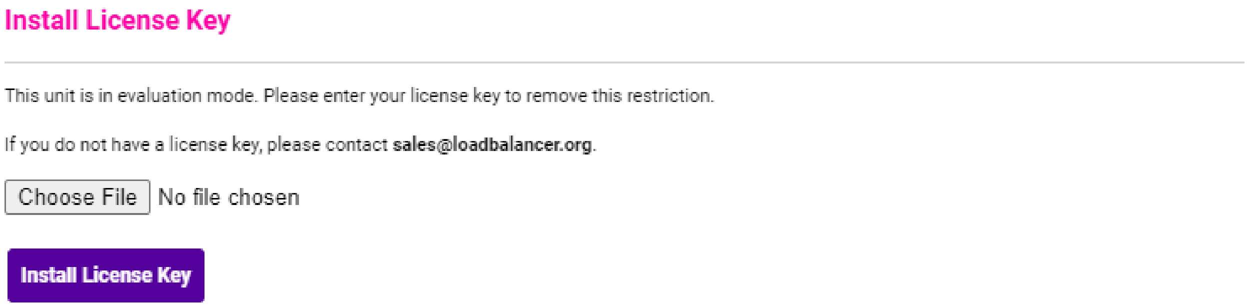
For an unlicensed hardware appliance, the following message is displayed:



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**.

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

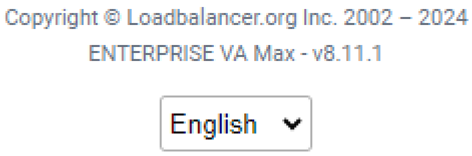
> **Note** Once the license is applied, these warning messages will no longer be displayed.

9.6. Appliance Software Update

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

9.6.1. Determining the Current Software Version

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

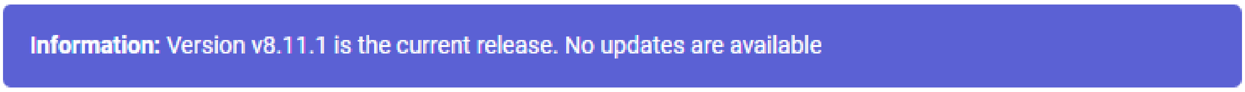


Copyright © Loadbalancer.org Inc. 2002 – 2024
ENTERPRISE VA Max - v8.11.1

9.6.2. 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:

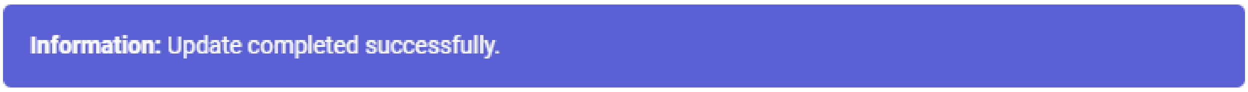


Information: Version v8.11.1 is the current release. No updates are available

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.

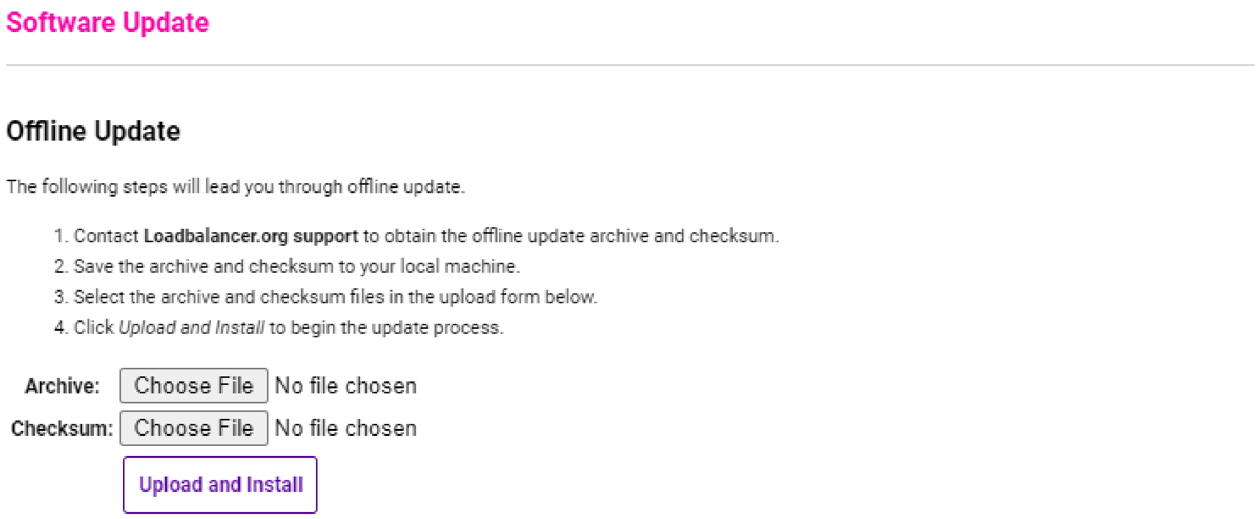
9.6.3. Using Offline Update

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

> **Note** Please contact support@loadbalancer.org 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: Choose File No file chosen

Checksum: Choose File 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.

9.7. Appliance Security Mode Configuration

To enable shell commands to be run from the WebUI and to enable SSH access, the appliance Security Mode must be configured:

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

2. Set *Appliance Security Mode* to **Custom**.

3. If SSH access is required, un-check *Disable SSH Password Access*.

4. Click **Update**.

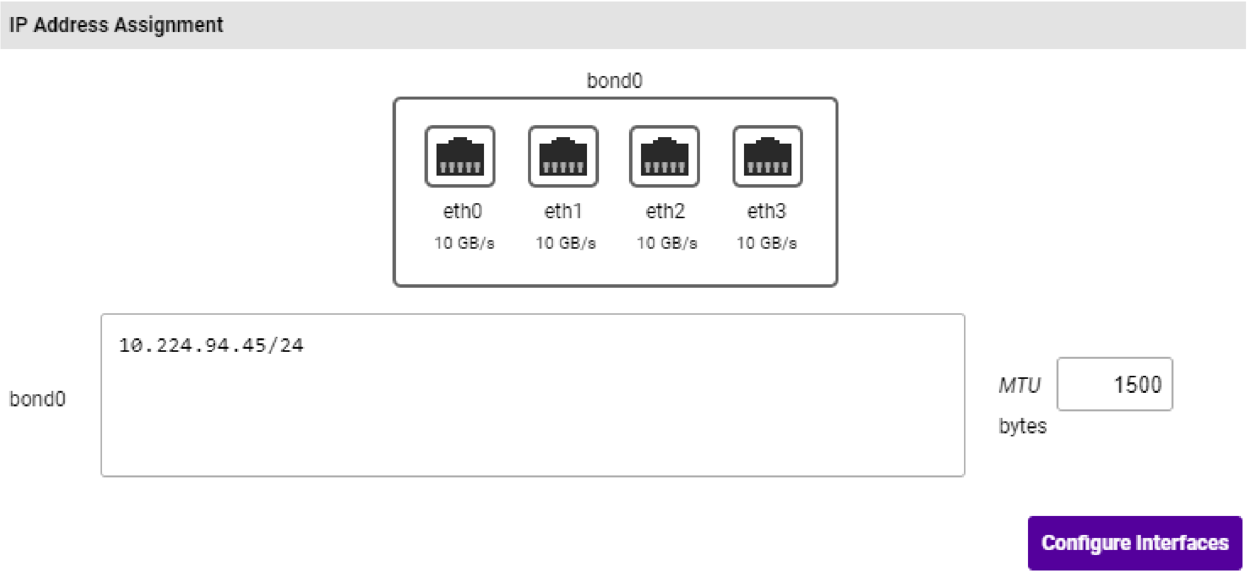
9.8. Appliance Network Configuration

The standard Vue PACS network configuration uses all 4 network adapters configured as an LACP 802.3ad bonded interface.

9.8.1. Verify Network Connections

1. Verify that all 4 network adapters are connected to the appropriate switch.

2. Using the WebUI, navigate to: *Local Configuration > Network Interface Configuration*.



IP Address Assignment

bond0: 10.224.94.45/24

MTU: 1500 bytes

3. Verify that the network is configured as required.

Note

The IP address/CIDR prefix for **bond0** was set during the Network Setup Wizard and will be shown here, e.g. **10.224.94.45/24**.

Note

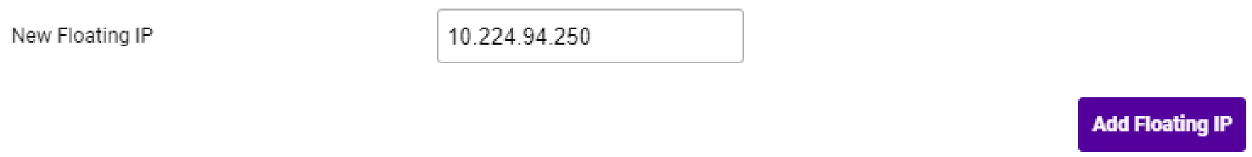
If you need to configure VLANs, modify the default gateway, configure static routes or configure

Policy Based Routing, please refer to the Appendix.

9.8.2. Configuring a floating IP Address for use as a Default Gateway

For layer 7 SNAT mode VIPs with TProxy (transparency) enabled, the load balancer must be the default gateway for the Real Servers. When using a clustered pair, a floating IP address must be used as the default gateway for the Real Servers to allow the gateway address to be brought up on either appliance. This should be a spare, unused IP in the same subnet as the Real Servers.

1. Using the Appliance WebUI, navigate to: *Cluster Configuration > Floating IPs*.
2. Enter the required address in the *New Floating IP* field, e.g. **10.224.94.250**.



New Floating IP 10.224.94.250

3. Click **Add Floating IP**.

Important

The default gateway for each Real Server associated with the following VIP must be configured to be this floating IP address:

- VIP 1 - **DICOM_VIP**

9.8.3. Configuring Hostname & DNS

1. Using the WebUI, navigate to: *Local Configuration > Hostname & DNS*.
2. Set the required *Hostname* and *Domain Name*.
3. Configure additional DNS servers if required.
4. Click **Update**.

9.8.4. Configuring NTP

1. Using the WebUI, navigate to: *Local Configuration > System Date & Time*.
2. Select the required *System Timezone*.
3. Navigate to the first field in the *NTP Servers* section, specify the IP address of an appropriate NTP server used at the site.
4. Click **Set Timezone & NTP**.

9.9. Configuring Load Balanced Vue PACS Services

Note

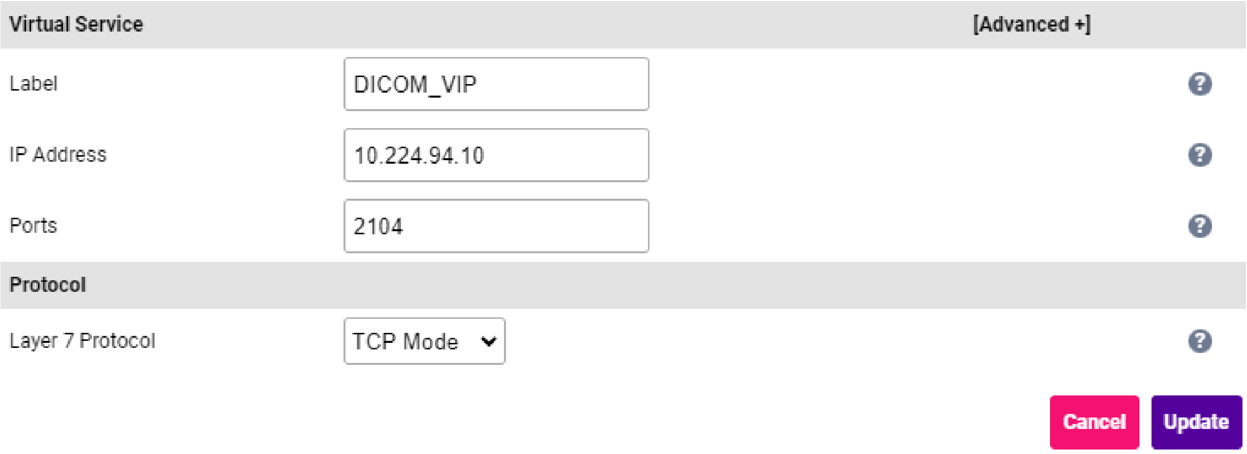
All Virtual Services are listed in the table in Virtual Services (VIP) Requirements.

9.9.1. VIP 1 - DICOM_VIP

9.9.1.1. Virtual Service (VIP) 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	DICOM_VIP
IP Address	10.224.94.10
Ports	2104
Protocol	
Layer 7 Protocol	TCP Mode

   - Specify an appropriate *Label* for the Virtual Service, e.g. **DICOM_VIP**.
   - Set the *Virtual Service IP Address* field to the required IP address, e.g. **10.224.94.10**.
   - Set the *Ports* field to **2104**.

> **Note**
>
> If additional ports are needed, use a comma between each port number, e.g. **104,2104**. If the associated Real Server's port is left blank, connections will be passed through on the same port. If a Real Server port is specified, e.g. **2104** all connections will be forwarded to that port.

   - Set the *Layer 7 Protocol* to **TCP Mode**.

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

4. Now click **Modify** next to the newly created VIP.

5. Scroll to the *Fallback Server* section.
   - Set the *IP Address* to the address of the Secondary WFM Server, e.g. **10.224.94.101**.
   - Set the *Port* to **2104**.

6. Scroll to the *Other* section and click **[Advanced]**.
   - Enable (check) the *Transparent Proxy* checkbox.

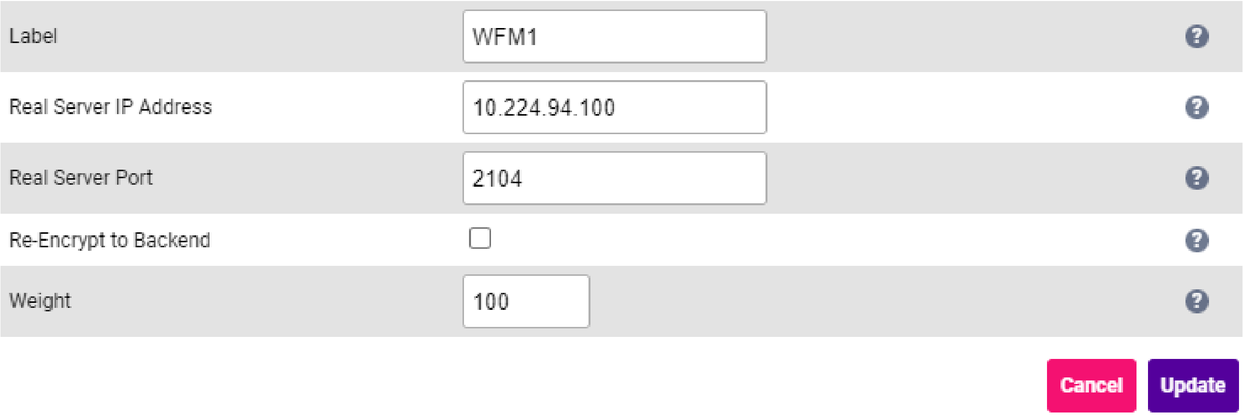
7. Leave all other settings at their default value.

8. Click **Update**.

9.9.1.2. Define the Associated Real Servers (RIPs)

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	WFM1
Real Server IP Address	10.224.94.100
Real Server Port	2104
Re-Encrypt to Backend	□
Weight	100

- Specify an appropriate *Label* for the RIP, e.g. **WFM1**.
- Set the *Real Server IP Address* field to address of the Primary WFM Server, e.g. **10.224.94.100**.
- Set the *Real Server Port* field to **2104**.

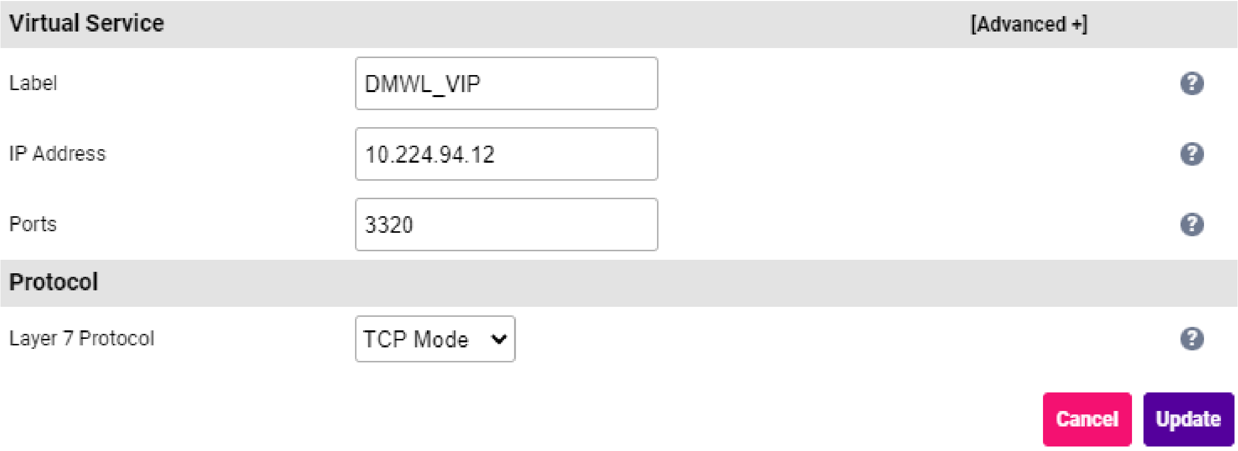
3. Leave all other settings at their default value.
4. Click **Update**.

> (!) Important — The default gateway of the primary and secondary WFM servers must be set to be the load balancer. Specify the floating IP address that was configured in Section 9.8.2.

9.9.2. VIP 2 - DMWL_VIP

9.9.2.1. Virtual Service (VIP) 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:



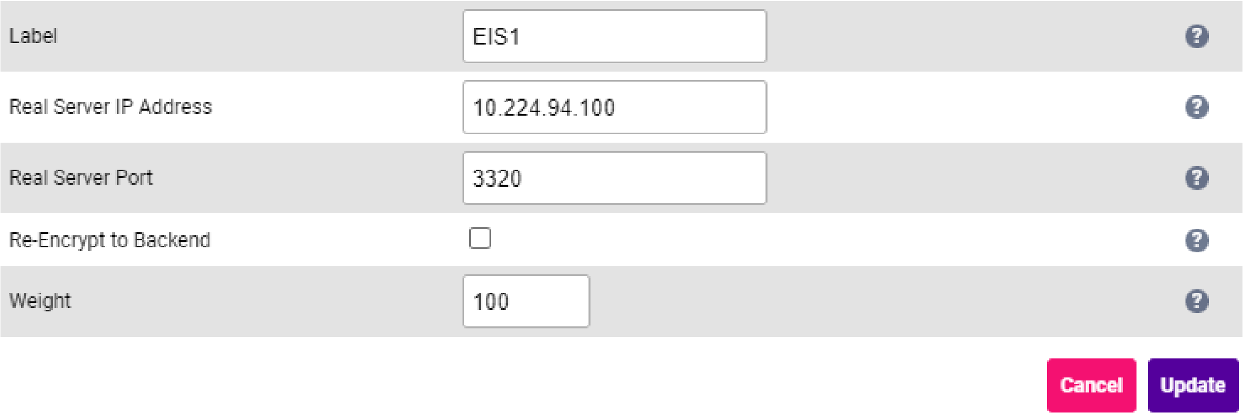
Virtual Service	[Advanced +]
Label	DMWL_VIP
IP Address	10.224.94.12
Ports	3320
Protocol	
Layer 7 Protocol	TCP Mode

- Specify an appropriate *Label* for the Virtual Service, e.g. **DMWL_VIP**.

    - Set the *Virtual Service IP Address* field to the required IP address, e.g. **10.224.94.12**.
    - Set the *Ports* field to **3320**.
    - Set the *Layer 7 Protocol* to **TCP Mode**.
3. Click **Update** to create the Virtual Service.
4. Now click **Modify** next to the newly created VIP.
5. Scroll to the *Other* section and click **[Advanced]**.
    - Enable (check) the *Timeout* checkbox.
    - Set *Client Timeout* and *Real Server Timeout* to **15m** (15 minutes).
6. Leave all other settings at their default value.
7. Click **Update**.

9.9.2.2. Define the Associated Real Servers (RIPs)

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	EIS1
Real Server IP Address	10.224.94.100
Real Server Port	3320
Re-Encrypt to Backend	☐
Weight	100

    - Specify an appropriate *Label* for the RIP, e.g. **EIS1**.
    - Set the *Real Server IP Address* field to address of the Primary EIS Server, e.g. **10.224.94.100**.
    - Set the *Real Server Port* field to **3320**.
3. Leave all other settings at their default value.
4. Repeat these steps to add the remaining EIS server(s)
5. Click **Update**.

9.9.3. VIP 3 - PORTAL_VIP

9.9.3.1. Configure the Custom Health Check

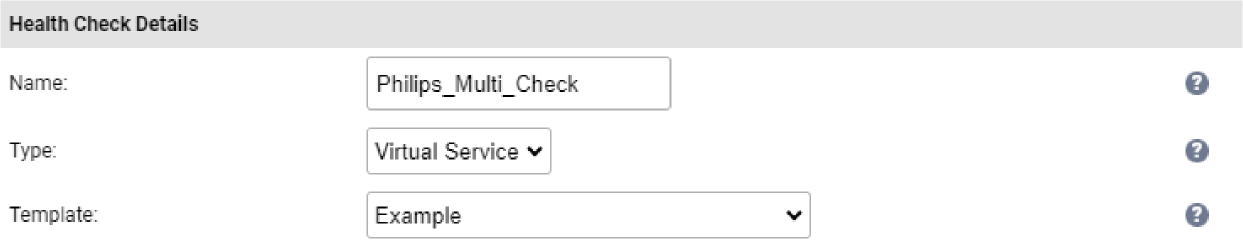
A custom health check is required to enable port 443 on the portal and also port 7070 or 11111 on the primary WFM to be checked. In this way, if the portal or the WFM port is down, automatic failover to the standby WFM will occur. The script is shown below:

```
#!/bin/bash
PATH=/usr/local/sbin:/usr/local/bin:/sbin:/bin:/usr/sbin:/usr/bin:/root/bin:/root/

# Variables passed to the health check script.
# $1 = VIP Address
# $2 = VIP Port
# $3 = Real Server IP
# $4 = Real Server Port

# Script Variables.
AGENT_IP="10.3.147.27"
AGENT_PORT="11111"
CHECK_PORTAL_URL="/portal/WebLogin.aspx?force_all_browsers=true"
CHECK_PORTAL_URL_RESPONSE=""
EXPECTED_PORTAL_URL_RESPONSE="200"
CHECK_TIMEOUT=5

nc -w $CHECK_TIMEOUT -zvn $AGENT_IP $AGENT_PORT &>/dev/null
AGENT_RESPONSE=$?

if [[ "$AGENT_RESPONSE" == "0" ]]
then
    if [[ $(curl -k -m $CHECK_TIMEOUT -o /dev/null -s -w "%{http_code}\n" https://$3:$4
/$CHECK_PORTAL_URL) == "$EXPECTED_PORTAL_URL_RESPONSE" ]]
    then
        ec=0
    else
        ec=20
    fi
else
    ec=10
fi
exit $ec
```

> Note
>
> The **AGENT_IP** and **AGENT_PORT** variables must be edited and set to the correct values.

To add this custom script to the load balancer:

1. Using the WebUI, navigate to *Cluster Configuration > Layer 7 – Health Check Scripts* and click **Add a new Virtual Service**.
2. Click **Add New Health Check**.
3. Enter the following details:



Health Check Details

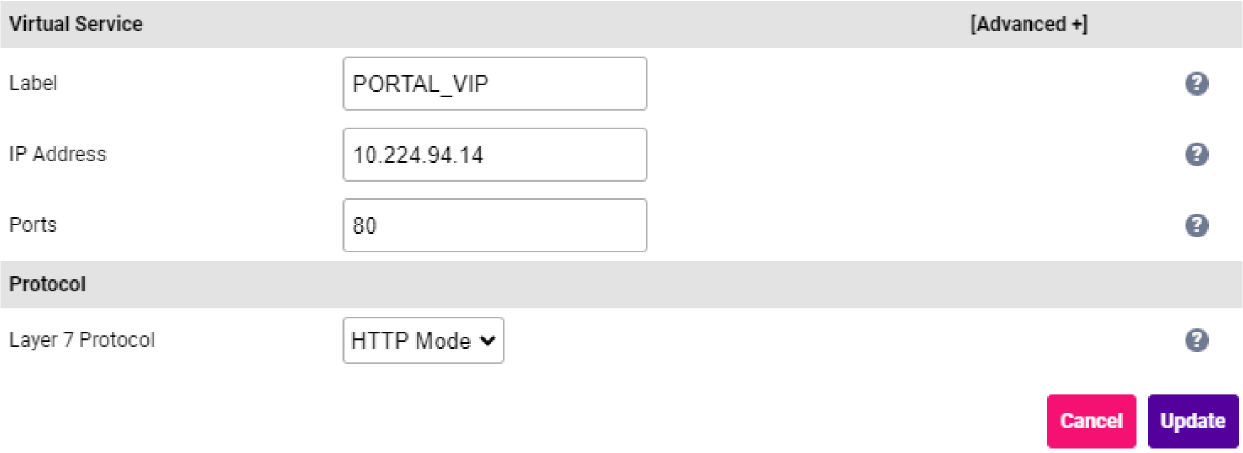
Name:	Philips_Multi_Check
Type:	Virtual Service
Template:	Example

- Set the *Name* to **Philips_Multi_Check**.
- Leave the *Type* drop-down set to **Virtual Service**.
- Copy the script above into the edit window over writing all current content.
- Set the **AGENT_IP** and **AGENT_PORT** variables to the correct values.

4. Click **Update** to save the new health check script.

9.9.3.2. Virtual Service (VIP) 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	PORTAL_VIP
IP Address	10.224.94.14
Ports	80
Protocol	
Layer 7 Protocol	HTTP Mode

- Specify an appropriate *Label* for the Virtual Service, e.g. **PORTAL_VIP**.
- Set the *Virtual Service IP Address* field to the required IP address, e.g. **10.224.94.14**.
- Set the *Ports* field to **80**.
- Set the *Layer 7 Protocol* to **HTTP Mode**.

3. Click **Update** to create the Virtual Service.
4. Now click **Modify** next to the newly created VIP.
5. Scroll to the *Protocol* section and click **[Advanced]**.
   - Enable (check) the *Reuse Idle HTTP Connections* checkbox.
6. Scroll to the *Fallback Server* section.
   - **If the standby site has a single portal server:**
     - Set the *IP Address* to the address of the standby portal server, e.g. **10.224.94.120**.
     - Set the *Port* to **80**.
   - **If the standby site has multiple portal servers:**
     - Set the *IP Address* to the address of VIP 4 (PORTAL_VIP_STANDY), e.g. **10.224.94.16**.

- Set the *Port* to **80**.

7. Scroll to the *Health Checks* section.
   - Set the *Check Type* to **External Script**.
   - Set the *Check Script* to the custom health check created previously, e.g. **Philips_Multi_Check**.
8. Scroll to the *ACL Rules* section.
9. Using the **Add Rule** button, add the following ACL rules:
   - **Rule 1**

```
Type:           path_beg
Bool:           Equals
URL/Text:       -m reg [^a-zA-Z]chat[^a-zA-Z]
Action:         Use Backend
Location/Value: CHAT
```

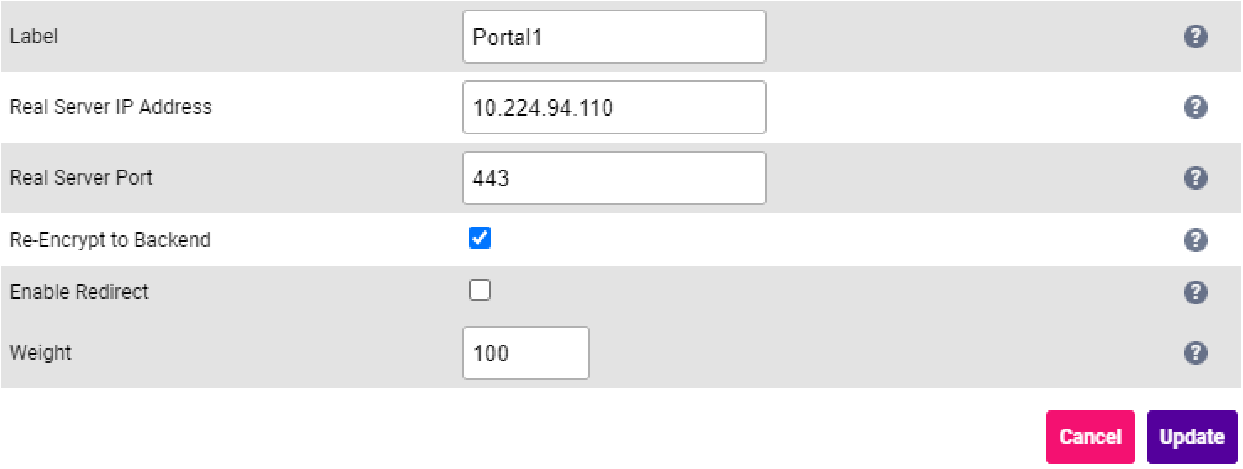
   - **Rule 2**

```
Type:           path_beg
Bool:           Equals
URL/Text:       -m reg [^a-zA-Z]syscfg[^a-zA-Z]
Action:         Use Backend
Location/Value: CHAT
```

10. Leave all other settings at their default value.
11. Click **Update**.

9.9.3.3. Define the Associated Real Servers (RIPs)

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	Portal1
Real Server IP Address	10.224.94.110
Real Server Port	443
Re-Encrypt to Backend	☑
Enable Redirect	☐
Weight	100

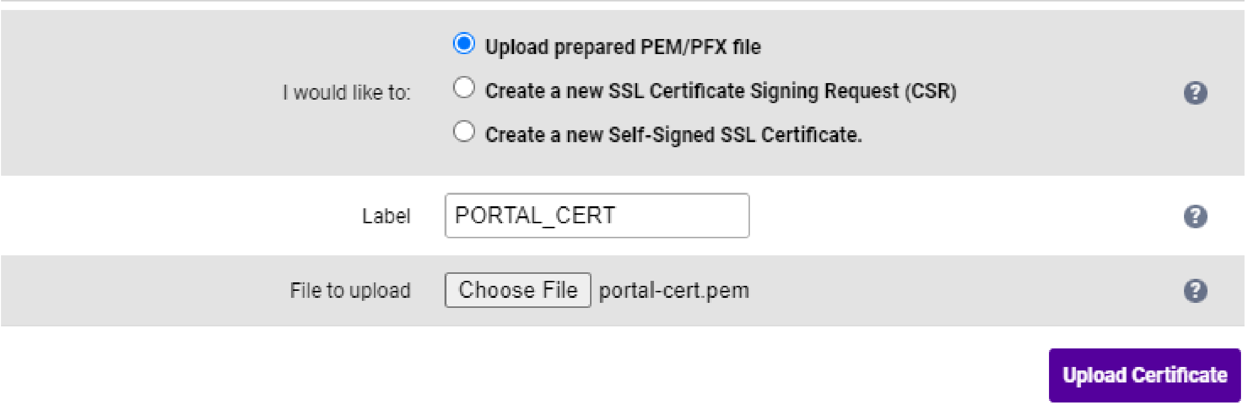
- Specify an appropriate *Label* for the RIP, e.g. **Portal1**.
- **If the primary site has a single portal server:**
  - Set the *Real Server IP Address* field to the address of the primary portal server, e.g. **10.224.94.110**.
  - Set the *Real Server Port* field to **443**.
  - Enable (check) *Re-Encrypt to Backend*.
  - Leave all other settings at their default value.
- **If the primary site has multiple portal servers:**
  - Set the *Real Server IP Address* field to the address of the first portal server, e.g. **10.224.94.110**.
  - Set the *Real Server Port* field to **443**.
  - Enable (check) *Re-Encrypt to Backend*.
  - Leave all other settings at their default value.
  - Repeat these steps to add the remaining portal server(s).

3. Click **Update**.

9.9.3.4. Upload the SSL Certificate

> ℹ Note
>
> If the production certificate is not currently available, continue to the next section (configuring SSL Termination) and leave *SSL Certificate* set to **Default Self Signed Certificate**. Once you have the production certificate, follow the steps in this section to upload the certificate and then navigate to *Cluster Configuration > SSL Termination*, click **Modify** next to the SSL termination, change *SSL Certificate* to the new certificate and click **Update**.

1. Using the WebUI, navigate to *Cluster Configuration > SSL Certificate* and click **Add a new SSL Certificate**.
2. Select the option **Upload prepared PEM/PFX file**.
3. Enter the following details:



I would like to:	● Upload prepared PEM/PFX file ○ Create a new SSL Certificate Signing Request (CSR) ○ Create a new Self-Signed SSL Certificate.
Label	PORTAL_CERT
File to upload	Choose File portal-cert.pem

- Specify an appropriate *Label*, e.g. **PORTAL_CERT**.
- Click **Choose File**.
- Browse to and select the relevant PEM or PFX file.

- For PFX files specify the password if required.

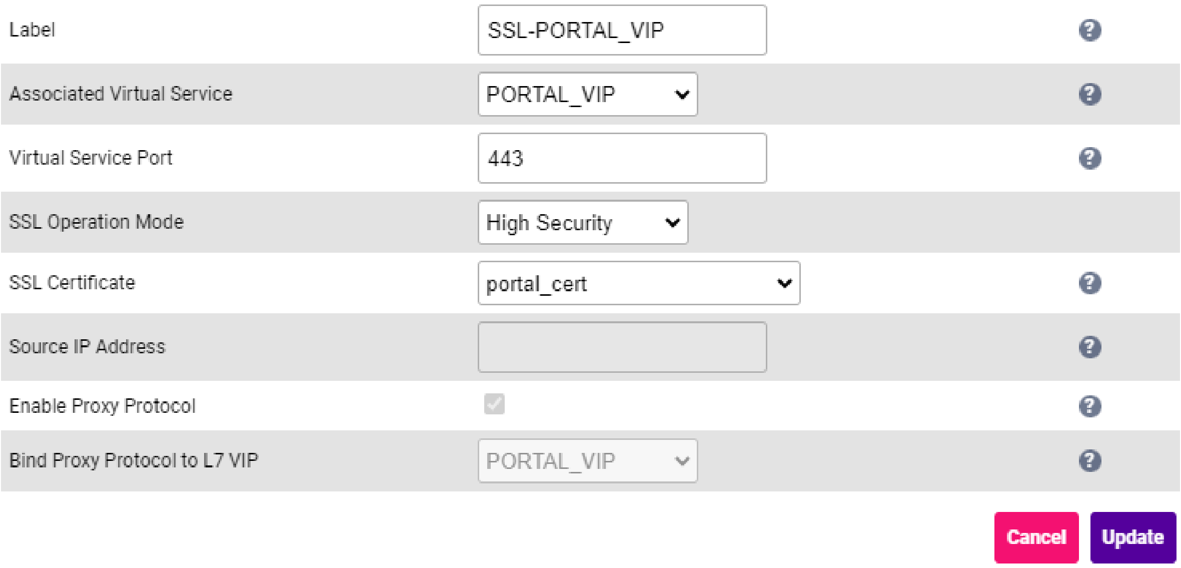
4. Click **Upload Certificate**.

> **Note** If you don't have a certificate and want to create a Certificate Signing Request (CSR) on the load balancer, please refer to Generating a CSR on the Load Balancer.

9.9.3.5. Configuring SSL Termination

1. Using the WebUI, navigate to *Cluster Configuration > SSL Termination* and click **Add a new Virtual Service**.

2. Enter the following details:



Label	SSL-PORTAL_VIP
Associated Virtual Service	PORTAL_VIP
Virtual Service Port	443
SSL Operation Mode	High Security
SSL Certificate	portal_cert
Source IP Address	
Enable Proxy Protocol	☑
Bind Proxy Protocol to L7 VIP	PORTAL_VIP

- Using the *Associated Virtual Service* drop-down, select the Virtual Service created previously, e.g. **PORTAL_VIP**.

> **Note** Once the VIP is selected, the *Label* field will be auto-populated with **SSL-PORTAL_VIP**. This can be changed if preferred.

- Ensure that the *Virtual Service Port* is set to **443**.
- Leave *SSL Operation Mode* set to **High Security**.
- Select the *SSL certificate* uploaded previously, e.g. **portal_cert**.

3. Leave all other settings at their default value.

4. Click **Update**.

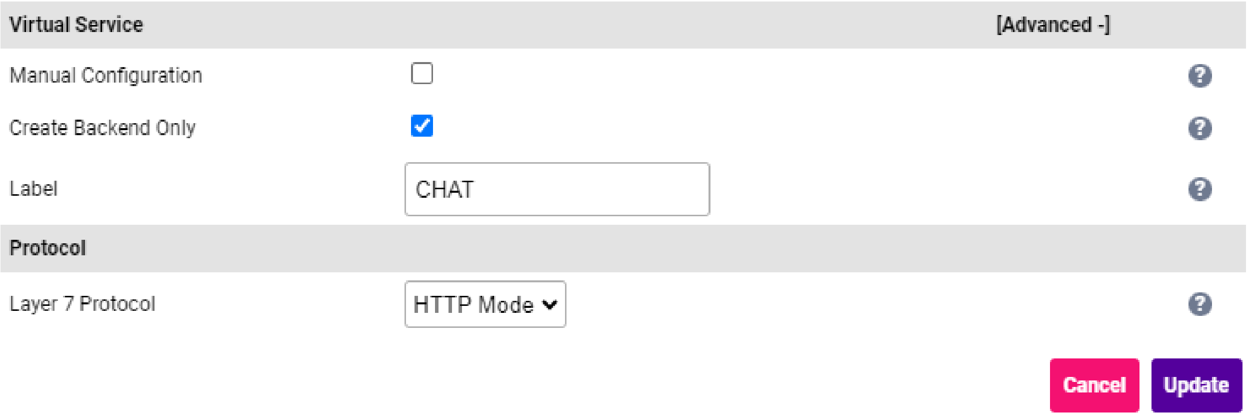
9.9.4. VIP 3-B1 - CHAT

9.9.4.1. Virtual Service (VIP) Configuration

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

2. Click **[Advanced]**.

3. Enter the following details:



Virtual Service	[Advanced -]
Manual Configuration	□
Create Backend Only	☑
Label	CHAT
Protocol	
Layer 7 Protocol	HTTP Mode

   - Select (Check) **Create Backend Only**.
   - Specify an appropriate *Label* for the Virtual Service, e.g. **CHAT**.
   - Set the *Layer 7 Protocol* to **HTTP Mode**.

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

5. Now click **Modify** next to the newly created VIP.

6. Scroll to the *Persistence* section.

   - Set *Persistence Mode* to **None**.

7. Scroll to the *Health Checks* section.

   - Set the *Check Type* to **Negotiate HTTPS (GET)**.

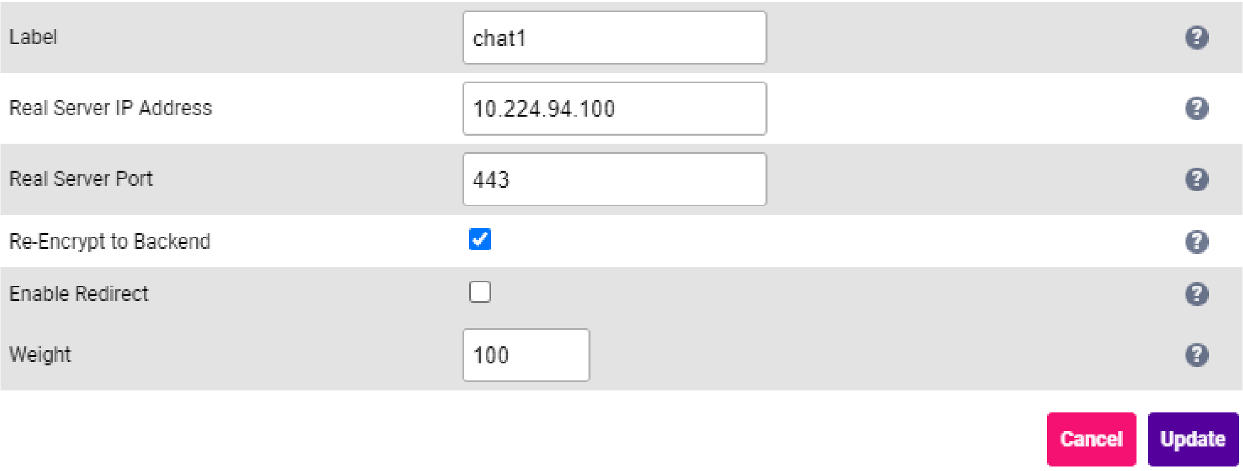
8. Leave all other settings at their default value.

9. Click **Update**.

9.9.4.2. Define the Associated Real Servers (RIPs)

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	chat1
Real Server IP Address	10.224.94.100
Real Server Port	443
Re-Encrypt to Backend	☑
Enable Redirect	□
Weight	100

- Specify an appropriate ***Label*** for the RIP, e.g. **chat1**.
- Set the *Real Server IP Address* field to address of the Primary WFM Server, e.g. **10.224.94.100**.
- Set the *Real Server Port* field to 443.

3. Leave all other settings at their default value.
4. Repeat these steps to add a second portal server.
5. Click **Update**.

9.9.4.3. Customize the Configuration

All chat and syscfg traffic should be handled by the primary portal server. If this server fails, the second portal server should take over. It's not currently possibly to define a fallback server directly in the WebUI for a backend only VIP, so a manual configuration is needed:

1. Using the WebUI, navigate to *View Configuration > Layer 7*.
2. Scroll down to the section that starts with "**Backend CHAT**".
3. Now copy the entire configuration for the VIP as shown below:

```
backend CHAT
    id 1220791148
    mode http
    balance leastconn
    option httpchk GET / HTTP/1.0
    acl :connection_via_termination always_false
    option http-keep-alive
    timeout http-request 5s
    option forwardfor
    timeout tunnel 1h
    option redispatch
    option abortonclose
    server Chat1 10.224.94.110:443 id 2  weight 100  check  check-ssl verify none inter 4000
rise 2  fall 2  slowstart 8000 minconn 0  maxconn 0  on-marked-down shutdown-sessions  ssl
verify none sni req.hdr(host)
    server Chat2 10.224.94.111:443 id 3  weight 100  check  check-ssl verify none inter 4000
rise 2  fall 2  slowstart 8000 minconn 0  maxconn 0  on-marked-down shutdown-sessions  ssl
verify none sni req.hdr(host)
```

4. Using the WebUI, navigate to *Cluster Configuration > Layer 7 – Virtual Services*.
5. Click **Modify** next to the **CHAT** VIP.
6. In the *Virtual Service* section at the top of the page, click **[Advanced]** and enable (check) the *Manual Configuration* checkbox.
7. Click **Update**.
8. Using the WebUI, navigate to *Cluster Configuration > Layer 7 - Manual Configuration*.
9. Paste the VIP's configuration into the edit window and add following text to the end of the last line:

```
backup
```

As shown in bold below:

```
backend CHAT
    id 1220791148
    mode http
    balance leastconn
    option httpchk GET / HTTP/1.0
    acl :connection_via_termination always_false
    option http-keep-alive
    timeout http-request 5s
    option forwardfor
    timeout tunnel 1h
    option redispatch
    option abortonclose
    server Chat1 10.224.94.110:443 id 2  weight 100  check  check-ssl verify none inter 4000
rise 2  fall 2  slowstart 8000 minconn 0  maxconn 0  on-marked-down shutdown-sessions  ssl
verify none sni req.hdr(host)
    server Chat2 10.224.94.111:443 id 3  weight 100  check  check-ssl verify none inter 4000
rise 2  fall 2  slowstart 8000 minconn 0  maxconn 0  on-marked-down shutdown-sessions  ssl
verify none sni req.hdr(host) backup
```

10. Click **Update**.

ℹ Note

Creating the VIP in the normal way and then converting it to a Manual Configuration ensures the VIP and associated Real Server(s) can be viewed in the appliance WebUI.

9.9.5. VIP 4 - PORTAL_VIP_STANDBY

ℹ Note

This VIP is only required when there is a secondary site and that site has multiple Portal servers. If the standby site has a single server VIP 4 is not needed.

9.9.5.1. Configure the Custom Health Check

A custom health check is required to enable port 443 on the portal AND also 7070 or 11111 to the primary WFM to be checked. In this way, if the portal or the WFM port (either 7070 or 11111) is down, automatic failover to the standby WFM will occur. The script is shown below:

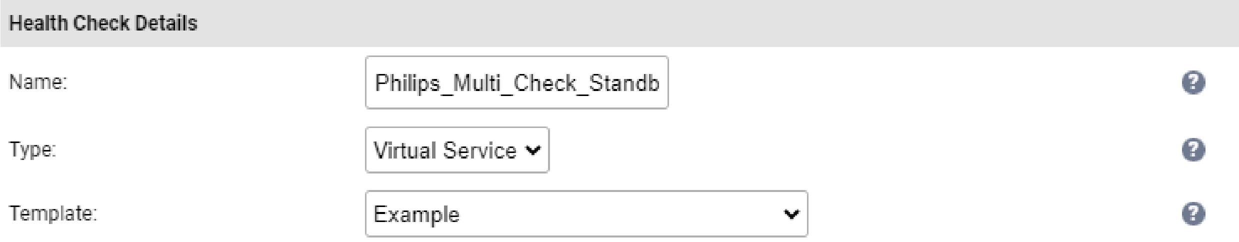
```
#!/bin/bash
PATH=/usr/local/sbin:/usr/local/bin:/sbin:/bin:/usr/sbin:/usr/bin:/root/bin:/root/

# Variables passed to the health check script.
# $1 = VIP Address
# $2 = VIP Port
# $3 = Real Server IP
# $4 = Real Server Port

# Script Variables.
AGENT_IP="10.3.147.27"
AGENT_PORT="11111"
CHECK_PORTAL_URL="/portal/WebLogin.aspx?force_all_browsers=true"
CHECK_PORTAL_URL_RESPONSE=""
EXPECTED_PORTAL_URL_RESPONSE="200"
CHECK_TIMEOUT=5
```

```
nc -w $CHECK_TIMEOUT -zvn $AGENT_IP $AGENT_PORT &>/dev/null
AGENT_RESPONSE=$?

if [[ "$AGENT_RESPONSE" == "0" ]]
then
    if [[ $(curl -k -m $CHECK_TIMEOUT -o /dev/null -s -w "%{http_code}\n" https://$3:$4
/$CHECK_PORTAL_URL) == "$EXPECTED_PORTAL_URL_RESPONSE" ]]
    then
        ec=0
    else
        ec=20
    fi
else
    ec=10
fi
exit $ec
```

> ℹ Note — The **AGENT_IP** and **AGENT_PORT** variables must be edited and set to the correct values.

To add this custom script to the load balancer:

1. Using the WebUI, navigate to *Cluster Configuration > Layer 7 – Health Check Scripts* and click **Add a new Virtual Service**.
2. Click **Add New Health Check**.
3. Enter the following details:



Health Check Details

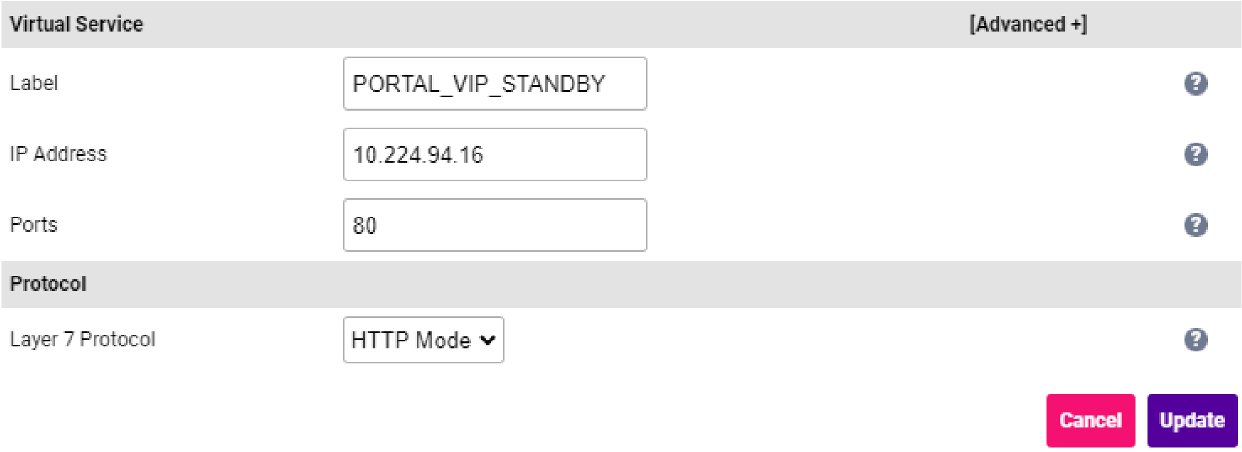
Name:	Philips_Multi_Check_Standb
Type:	Virtual Service
Template:	Example

   - Set the *Name* to **Philips_Multi_Check_Standby**.
   - Leave the *Type* drop-down set to **Virtual Service**.
   - Copy the script above into the edit window over writing all current content.
   - Set the *AGENT_IP* and *AGENT_PORT* variables to the correct values.

4. Click **Update** to save the new health check script.

9.9.5.2. Virtual Service (VIP) 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	PORTAL_VIP_STANDBY
IP Address	10.224.94.16
Ports	80

Protocol

Layer 7 Protocol	HTTP Mode

- Specify an appropriate *Label* for the Virtual Service, e.g. **PORTAL_VIP_STANDBY**.
- Set the *Virtual Service IP Address* field to the required IP address, e.g. **10.224.94.16**.
- Set the *Ports* field to **80**.
- Set the *Layer 7 Protocol* to **HTTP Mode**.

3. Click **Update** to create the Virtual Service.
4. Now click **Modify** next to the newly created VIP.
5. Scroll to the *Protocol* section and click **[Advanced]**.
   - Enable (check) the *Reuse Idle HTTP Connections* checkbox.
6. Scroll to the *Health Checks* section.
   - Set the *Check Type* to **External Script**.
   - Set the *Check Script* to the custom health check created previously, e.g. **Philips_Multi_Check_Standby**.
7. Scroll to the *ACL Rules* section.
8. Using the **Add Rule** button, add the following ACL rules:
   - **Rule 1**

```
Type:           path_beg
Bool:           Equals
URL/Text:       -m reg [^a-zA-Z]chat[^a-zA-Z]
Action:         Use Backend
Location/Value: CHAT_STANDBY
```

   - **Rule 2**

```
Type:           path_beg
Bool:           Equals
URL/Text:       -m reg [^a-zA-Z]syscfg[^a-zA-Z]
Action:         Use Backend
Location/Value: CHAT_STANDBY
```

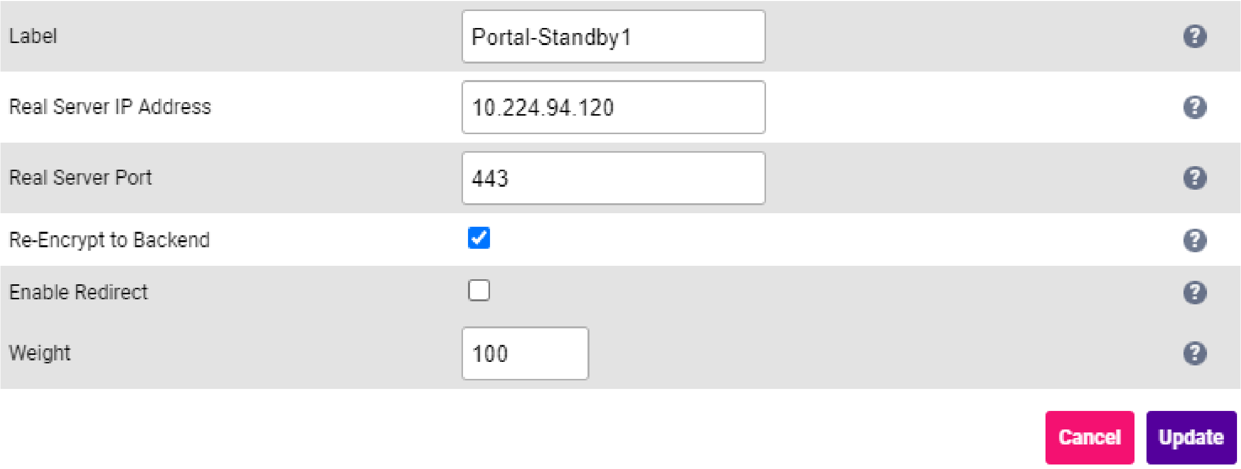
9. Leave all other settings at their default value.

10. Click **Update**.

9.9.5.3. Define the Associated Real Servers (RIPs)

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	Portal-Standby1
Real Server IP Address	10.224.94.120
Real Server Port	443
Re-Encrypt to Backend	☑
Enable Redirect	□
Weight	100

- Specify an appropriate *Label* for the RIP, e.g. **Portal-Standby1**.
- **If the standby site has a single portal server:**
  - Set the *Real Server IP Address* field to the address of the primary portal server, e.g. **10.224.94.115**.
  - Set the *Real Server Port* field to **443**.
  - Enable (check) *Re-Encrypt to Backend*.
  - Leave all other settings at their default value.
- **If the standby site has multiple portal servers:**
  - Set the *Real Server IP Address* field to the address of the first portal server, e.g. **10.224.94.115**.
  - Set the *Real Server Port* field to **443**.
  - Enable (check) *Re-Encrypt to Backend*.
  - Leave all other settings at their default value.
  - Repeat these steps to add the remaining portal server(s).

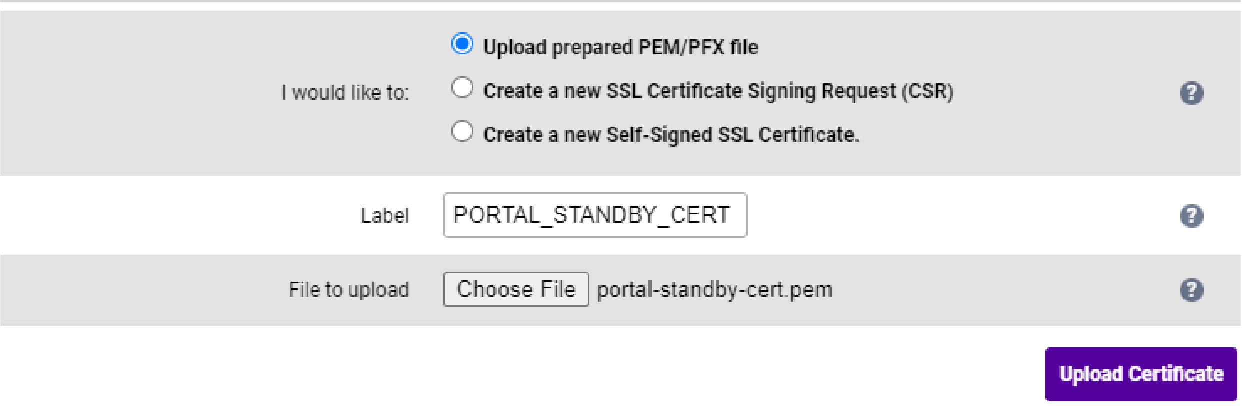
3. Click **Update**.

9.9.5.4. Upload the SSL Certificate

Note

If the production certificate is not currently available, continue to the next section (configuring SSL Termination) and leave *SSL Certificate* set to **Default Self Signed Certificate**. Once you have the production certificate, follow the steps in this section to upload the certificate and then navigate to *Cluster Configuration > SSL Termination*, click **Modify** next to the SSL termination, change *SSL Certificate* to the new certificate and click **Update**.

1. Using the WebUI, navigate to *Cluster Configuration > SSL Certificate* and click **Add a new SSL Certificate**.
2. Select the option **Upload prepared PEM/PFX file**.
3. Enter the following details:



I would like to:
● Upload prepared PEM/PFX file
○ Create a new SSL Certificate Signing Request (CSR)
○ Create a new Self-Signed SSL Certificate.

Label: PORTAL_STANDBY_CERT

File to upload: portal-standby-cert.pem

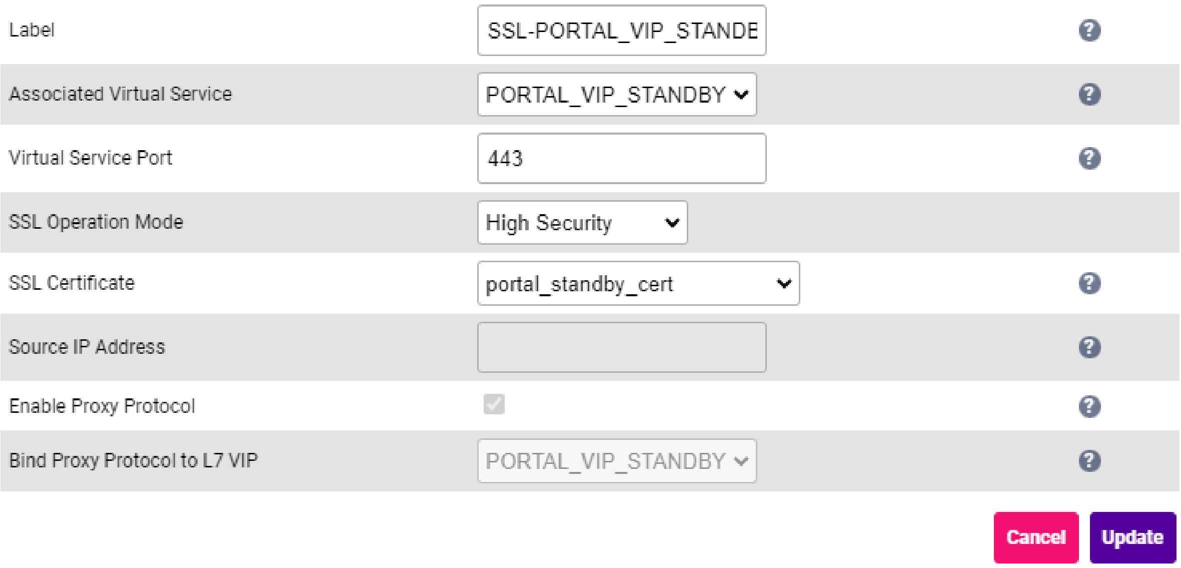
   - Specify an appropriate *Label*, e.g. **PORTAL_STANDBY_CERT**.
   - Click **Choose File**.
   - Browse to and select the relevant PEM or PFX file.
   - For PFX files specify the password if required.

4. Click **Upload Certificate**.

Note: If you don't have a certificate and want to create a Certificate Signing Request (CSR) on the load balancer, please refer to Generating a CSR on the Load Balancer.

9.9.5.5. Configuring SSL Termination

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



Label	SSL-PORTAL_VIP_STANDE
Associated Virtual Service	PORTAL_VIP_STANDBY
Virtual Service Port	443
SSL Operation Mode	High Security
SSL Certificate	portal_standby_cert
Source IP Address	
Enable Proxy Protocol	☑
Bind Proxy Protocol to L7 VIP	PORTAL_VIP_STANDBY

- Using the *Associated Virtual Service* drop-down, select the Virtual Service created previously, e.g. **PORTAL_VIP_STANDBY**.

> ℹ Note
>
> Once the VIP is selected, the *Label* field will be auto-populated with **SSL-PORTAL_VIP_STANDBY**. This can be changed if preferred.

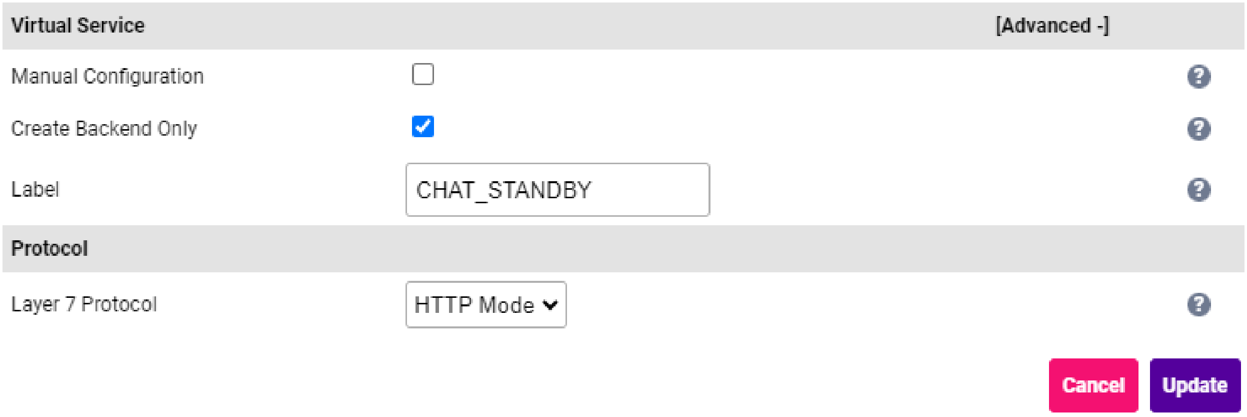
- Ensure that the *Virtual Service Port* is set to **443**.
- Leave *SSL Operation Mode* set to **High Security**.
- Select the *SSL certificate* uploaded previously, e.g. **portal_cert**.

3. Leave all other settings at their default value.
4. Click **Update**.

9.9.6. VIP 4-B1 - CHAT_STANDBY

9.9.6.1. Virtual Service (VIP) Configuration

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



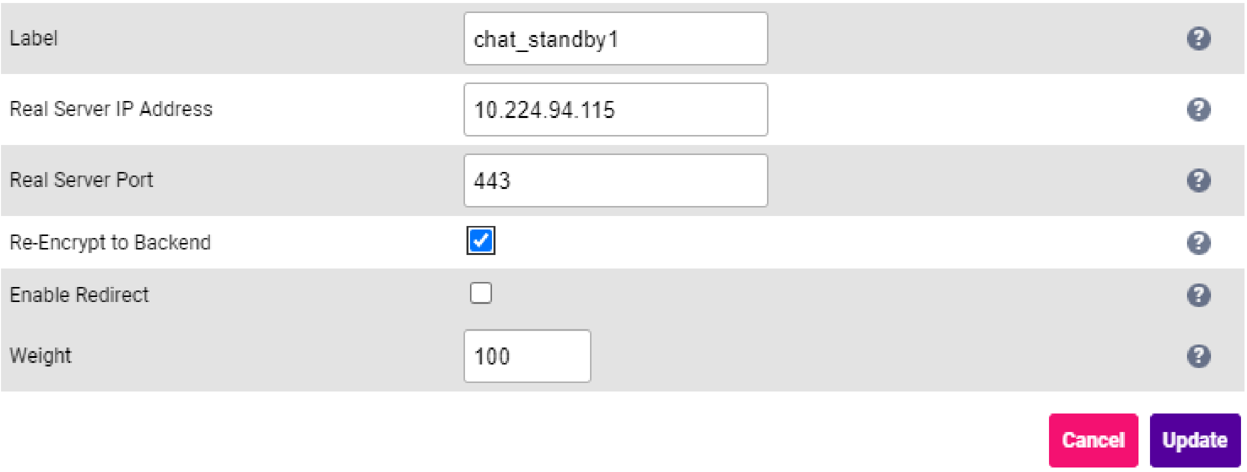
Virtual Service		**[Advanced -]**
Manual Configuration	☐	?
Create Backend Only	☑	?
Label	CHAT_STANDBY	?
Protocol		
Layer 7 Protocol	HTTP Mode	?

- Select (Check) **Create Backend Only**.
- Specify an appropriate *Label* for the Virtual Service, e.g. **CHAT_STANDBY**.
- Set the *Layer 7 Protocol* to **HTTP Mode**.

4. Click **Update** to create the Virtual Service.
5. Now click **Modify** next to the newly created VIP.
6. Scroll to the *Persistence* section.
   - Set *Persistence Mode* to **None**.
7. Scroll to the *Health Checks* section.
   - Set the *Check Type* to **Negotiate HTTPS (GET)**.
8. Leave all other settings at their default value.
9. Click **Update**.

9.9.6.2. Define the Associated Real Servers (RIPs)

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	chat_standby1	?
Real Server IP Address	10.224.94.115	?
Real Server Port	443	?
Re-Encrypt to Backend	☑	?
Enable Redirect	☐	?
Weight	100	?

- Specify an appropriate *Label* for the RIP, e.g. **chat_standby1**.
- Set the *Real Server IP Address* field to address of the standby WFM Server, e.g. **10.224.94.115**.
- Set the *Real Server Port* field to 443.

3. Leave all other settings at their default value.
4. Repeat these steps to add a second portal server.
5. Click **Update**.

9.9.6.3. Customize the Configuration

All chat and syscfg traffic should be handled by the primary portal server. If this server fails, the second portal server should take over. It's not currently possibly to define a fallback server directly in the WebUI for a backend only VIP, so a manual configuration is needed:

1. Using the WebUI, navigate to *View Configuration > Layer 7*.
2. Scroll down to the section that starts with "**Backend CHAT_STANDBY**".
3. Now copy the entire configuration for the VIP as shown below:

```
backend CHAT_STANDBY
    id 1220791148
    mode http
    balance leastconn
    option httpchk GET / HTTP/1.0
    acl :connection_via_termination always_false
    option http-keep-alive
    timeout http-request 5s
    option forwardfor
    timeout tunnel 1h
    option redispatch
    option abortonclose
    server Chat1 10.224.94.115:443 id 2  weight 100  check  check-ssl verify none inter 4000  rise 2  fall 2  slowstart 8000 minconn 0  maxconn 0  on-marked-down shutdown-sessions  ssl  verify none sni req.hdr(host)
    server Chat2 10.224.94.116:443 id 3  weight 100  check  check-ssl verify none inter 4000  rise 2  fall 2  slowstart 8000 minconn 0  maxconn 0  on-marked-down shutdown-sessions  ssl  verify none sni req.hdr(host)
```

4. Using the WebUI, navigate to *Cluster Configuration > Layer 7 – Virtual Services*.
5. Click **Modify** next to the **CHAT** VIP.
6. In the *Virtual Service* section at the top of the page, click **[Advanced]** and enable (check) the *Manual Configuration* checkbox.
7. Click **Update**.
8. Using the WebUI, navigate to *Cluster Configuration > Layer 7 - Manual Configuration*.
9. Paste the VIP's configuration into the edit window and add following text to the end of the last line:

```
backup
```

As shown in bold below:

```
backend CHAT_STANDBY
    id 1220791148
    mode http
    balance leastconn
    option httpchk GET / HTTP/1.0
    acl :connection_via_termination always_false
    option http-keep-alive
    timeout http-request 5s
    option forwardfor
    timeout tunnel 1h
    option redispatch
    option abortonclose
    server Chat1 10.224.94.110:443 id 2  weight 100  check  check-ssl verify none inter 4000
rise 2  fall 2  slowstart 8000 minconn 0  maxconn 0  on-marked-down shutdown-sessions  ssl
verify none sni req.hdr(host)
    server Chat2 10.224.94.111:443 id 3  weight 100  check  check-ssl verify none inter 4000
rise 2  fall 2  slowstart 8000 minconn 0  maxconn 0  on-marked-down shutdown-sessions  ssl
verify none sni req.hdr(host) backup
```

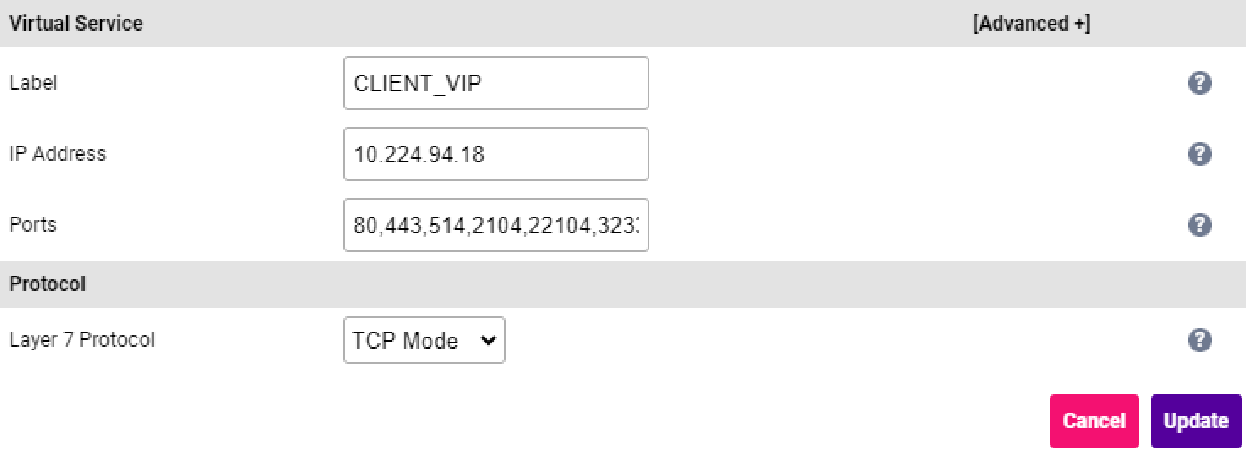
10. Click **Update**.

Note: Creating the VIP in the normal way and then converting it to a Manual Configuration ensures the VIP and associated Real Server(s) can be viewed in the appliance WebUI.

9.9.7. VIP 5 - CLIENT_VIP

9.9.7.1. Virtual Service (VIP) 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	
Label	CLIENT_VIP
IP Address	10.224.94.18
Ports	80,443,514,2104,22104,323
Protocol	
Layer 7 Protocol	TCP Mode

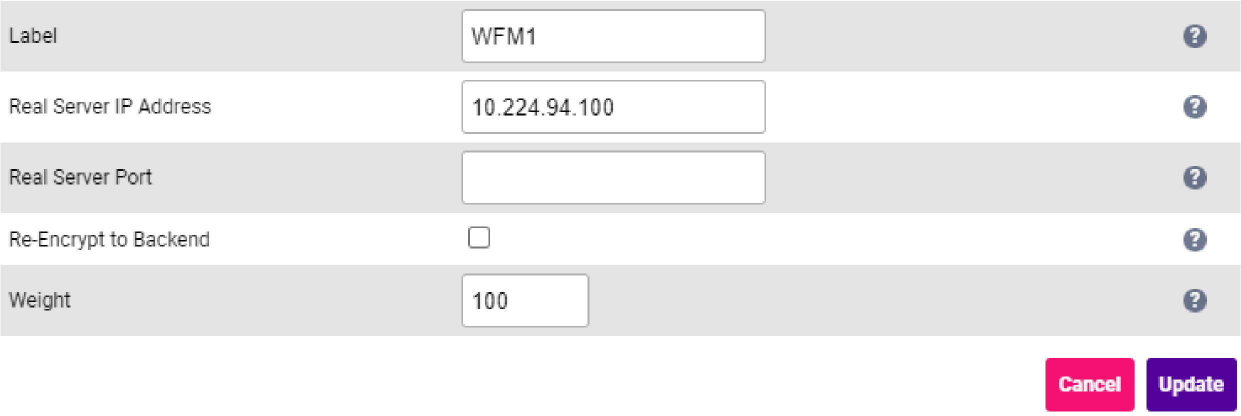
- Specify an appropriate *Label* for the Virtual Service, e.g. **CLIENT_VIP**.
- Set the *Virtual Service IP Address* field to the required IP address, e.g. **10.224.94.18**.

- Set the *Ports* field to **80,443,514,2104,22104,32338**.
- Set the *Layer 7 Protocol* to **TCP Mode**.

3. Click **Update** to create the Virtual Service.
4. Now click **Modify** next to the newly created VIP.
5. Scroll to the *Fallback Server* section.
   - Set the *IP Address* to the address of the Secondary WFM Server, e.g. **10.224.94.101**.
   - Ensure that the *Port* field is left blank.
6. Leave all other settings at their default value.
7. Click **Update**.

9.9.7.2. Define the Associated Real Servers (RIPs)

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	WFM1
Real Server IP Address	10.224.94.100
Real Server Port	
Re-Encrypt to Backend	☐
Weight	100

   - Specify an appropriate *Label* for the RIP, e.g. **WFM1**.
   - Set the *Real Server IP Address* field to address of the Primary WFM Server, e.g. **10.224.94.100**.
   - Leave the *Real Server Port* field blank.
3. Leave all other settings at their default value.
4. Click **Update**.

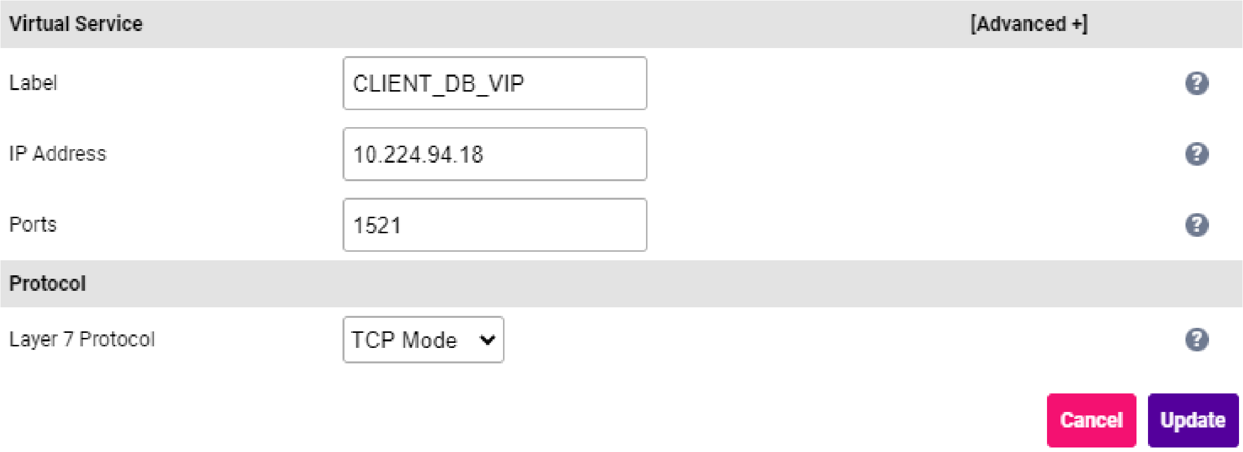
9.9.8. VIP 6 - CLIENT_DB_VIP

> Note
>
> This VIP is is only needed for ***Infoscaler/Veritas*** implementations where the backend is made up of 2 core nodes - 1 running the application and 1 running the DB.

9.9.8.1. Virtual Service (VIP) 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:



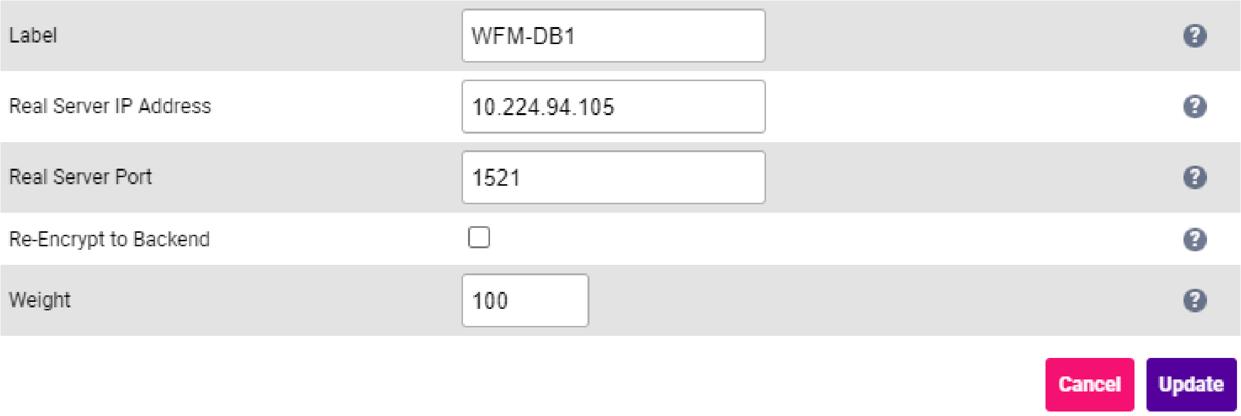
Virtual Service	[Advanced +]
Label	CLIENT_DB_VIP
IP Address	10.224.94.18
Ports	1521
Protocol	
Layer 7 Protocol	TCP Mode

- Specify an appropriate *Label* for the Virtual Service, e.g. **CLIENT_DB_VIP**.
- Set the *Virtual Service IP Address* field to the required IP address, e.g. **10.224.94.20**.
- Set the *Ports* field to **1521**.
- Set the *Layer 7 Protocol* to **TCP Mode**.

3. Click **Update** to create the Virtual Service.
4. Now click **Modify** next to the newly created VIP.
5. Scroll to the *Fallback Server* section.
   - Set the *IP Address* to the address of the Secondary WFM-DB Server, e.g. **10.224.94.106**.
   - Set the *Port* field to **1521**.
6. Scroll to the *Other* section and click **[Advanced]**.
   - Enable (check) the *Timeout* checkbox.
   - Set *Client Timeout* and *Real Server Timeout* to **15m** (15 minutes).
7. Leave all other settings at their default value.
8. Click **Update**.

9.9.8.2. Define the Associated Real Servers (RIPs)

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	WFM-DB1
Real Server IP Address	10.224.94.105
Real Server Port	1521
Re-Encrypt to Backend	□
Weight	100

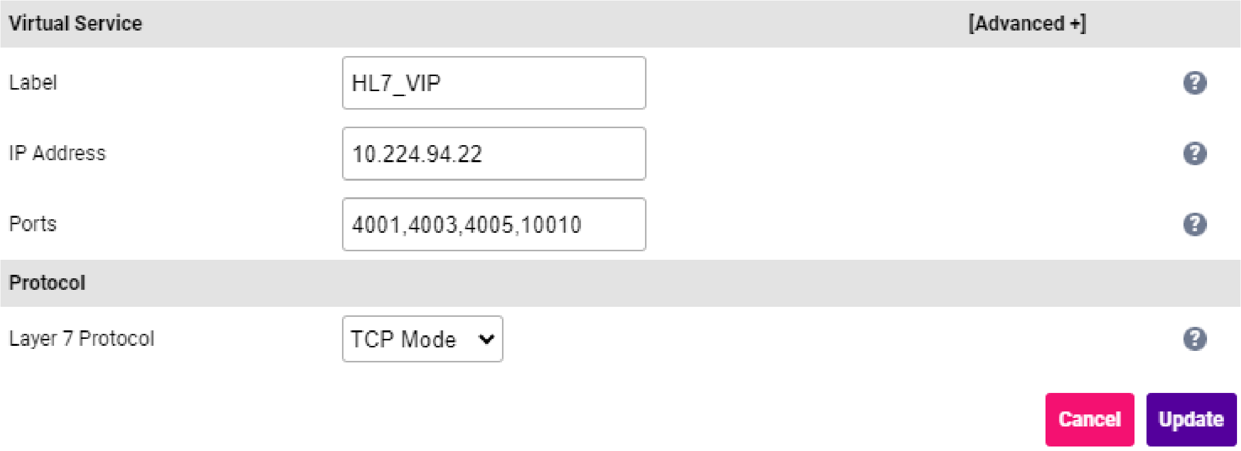
- Specify an appropriate *Label* for the RIP, e.g. **WFM-DB1**.
- Set the *Real Server IP Address* field to address of the Primary WFM-DB Server, e.g. **10.224.94.105**.
- Set the *Real Server Port* field to **1521**.

3. Leave all other settings at their default value.
4. Click **Update**.

9.9.9. VIP 7 - HL7_VIP

9.9.9.1. Virtual Service (VIP) 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	HL7_VIP
IP Address	10.224.94.22
Ports	4001,4003,4005,10010
Protocol	
Layer 7 Protocol	TCP Mode

- Specify an appropriate *Label* for the Virtual Service, e.g. **HL7_VIP**.
- Set the *Virtual Service IP Address* field to the required IP address, e.g. **10.224.94.22**.
- Set the *Ports* field to **4001,4003,4005,10010**.

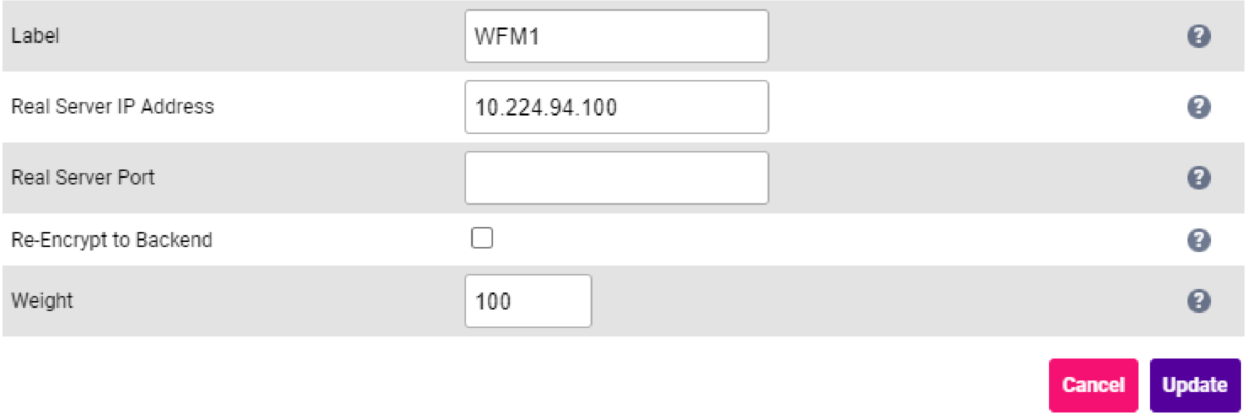
> Note
>
> The ports required are site specific, please verify that the port list is correct for the particular site.

- Set the *Layer 7 Protocol* to **TCP Mode**.

3. Click **Update** to create the Virtual Service.
4. Now click **Modify** next to the newly created VIP.
5. Scroll to the *Fallback Server* section.
   - Set the *IP Address* to the address of the Secondary WFM Server, e.g. **10.224.94.101**.
   - Ensure that the *Port* field is left blank.
6. Scroll to the *Other* section and click **[Advanced]**.
   - Enable (check) the *Timeout* checkbox.
   - Set *Client Timeout* and *Real Server Timeout* to **15m** (15 minutes).
7. Leave all other settings at their default value.
8. Click **Update**.

9.9.9.2. Define the Associated Real Servers (RIPs)

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	WFM1
Real Server IP Address	10.224.94.100
Real Server Port	
Re-Encrypt to Backend	□
Weight	100

   - Specify an appropriate *Label* for the RIP, e.g. **WFM1**.
   - Set the *Real Server IP Address* field to address of the Primary WFM Server, e.g. **10.224.94.100**.
   - Leave the *Real Server Port* field blank.

3. Leave all other settings at their default value.
4. Click **Update**.

9.9.9.3. Customize the Configuration

HL7 connections are typically established in the morning and stay connected throughout the day. When a failover from primary to standby occurs, this connection is moved to the standby server. However, with the default configuration, when the primary is made active again, the active session is NOT disconnected and moved back to the primary server. The HL7 VIP requires a custom configuration to force this:

1. Using the WebUI, navigate to *View Configuration > Layer 7*.
2. Scroll down to the section that starts with "**listen HL7_VIP**".
3. Now copy the entire configuration for the VIP as shown below:

```
listen HL7_VIP
    bind 10.224.94.22:4001,10.224.94.22:4003 transparent
    bind 10.224.94.22:4005,10.224.94.22:10010 transparent
    id 969879036
    mode tcp
    balance leastconn
    stick on src
    stick-table type ip size 10240k expire 30m peers loadbalancer_replication
    server backup 10.224.94.101: backup  non-stick
    timeout client 15m
    timeout server 15m
    acl :connection_via_termination always_false
    option redispatch
    option abortonclose
    maxconn 40000
    option tcplog
    server WFM1 10.224.94.100 id 2  weight 100  check port 4001 inter 4000  rise 2  fall 2
slowstart 8000 minconn 0  maxconn 0  on-marked-down shutdown-sessions
```

4. Using the WebUI, navigate to *Cluster Configuration > Layer 7 – Virtual Services*.
5. Click **Modify** next to **HL7_VIP**.
6. In the *Virtual Service* section at the top of the page, click **[Advanced]** and enable (check) the *Manual Configuration* checkbox.
7. Click **Update**.
8. Using the WebUI, navigate to *Cluster Configuration > Layer 7 - Manual Configuration*.
9. Paste the VIP's configuration into the edit window and add following text to the end of the last line:

```
on-marked-up shutdown-backup-sessions
```

As shown in bold below:

```
listen HL7_VIP
    bind 10.224.94.22:4001,10.224.94.22:4003 transparent
    bind 10.224.94.22:4005,10.224.94.22:10010 transparent
    id 969879036
    mode tcp
    balance leastconn
    stick on src
    stick-table type ip size 10240k expire 30m peers loadbalancer_replication
    server backup 10.224.94.101: backup  non-stick
    timeout client 15m
    timeout server 15m
    acl :connection_via_termination always_false
    option redispatch
    option abortonclose
    maxconn 40000
    option tcplog
    server WFM1 10.224.94.100 id 2  weight 100  check port 4001 inter 4000  rise 2  fall 2 slowstart 8000 minconn 0  maxconn 0  on-marked-down shutdown-sessions on-marked-up shutdown-backup-sessions
```

10. Click **Update**.

> Note
>
> Creating the VIP in the normal way and then converting it to a Manual Configuration ensures the VIP and associated Real Server(s) can be viewed in the appliance WebUI.

9.9.10. Finalizing the Configuration

To apply the new settings, HAProxy & STunnel 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**.
3. Click **Reload STunnel**.

10. Outbound (Iexport) configuration

For layer 7 VIPs, the source IP address of outbound packets from the load balancer to the Real Server is the interface IP address by default. For the configuration presented in this guide, this will be the IP address assigned to **bond0**.

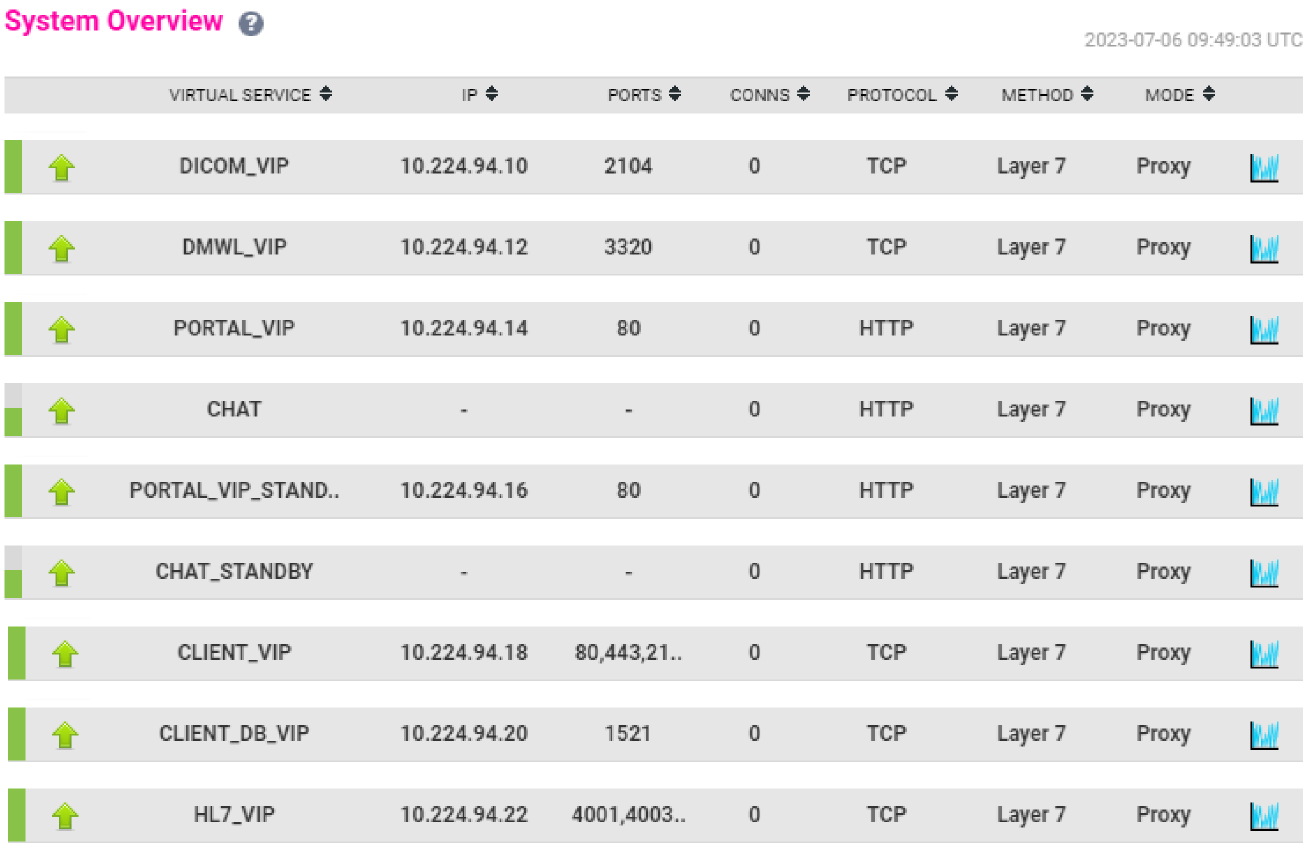
This can be changed if required - to the VIP address for example by following the steps below.

1. Using the WebUI, navigate to ***Cluster Configuration > Layer 7 – Virtual Services***.
2. Click **Modify** next to relevant VIP.
3. Scroll down to the ***Other*** section and click **[Advanced]**.
4. Enter the required IP address in the ***Set Source Address*** field.
5. Click **Update**.

11. Testing & Verification

> Note
>
> For additional guidance on diagnosing and resolving any issues you may have, please also refer to Diagnostics & Troubleshooting.

The System Overview can be accessed via the WebUI. It shows a graphical view of all VIPs & RIPs (i.e. the Vue PACS servers) and shows the state/health of each server as well as the state of each cluster as a whole. The example below shows that all Vue PACS servers are healthy (green) and available to accept connections:

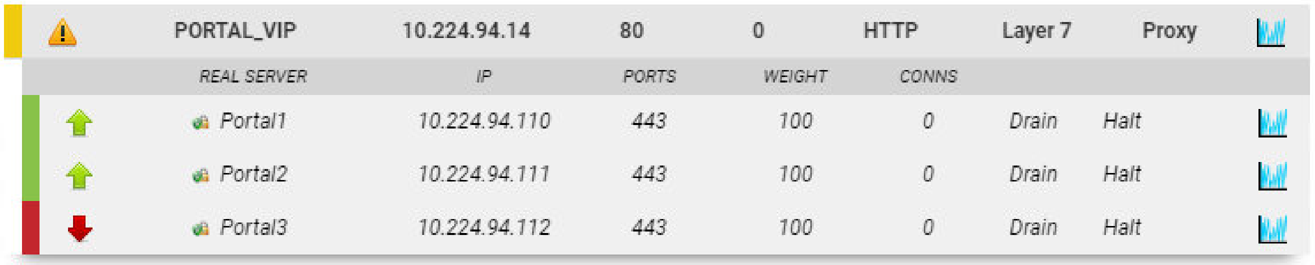


System Overview

2023-07-06 09:49:03 UTC

	VIRTUAL SERVICE	IP	PORTS	CONNS	PROTOCOL	METHOD	MODE
⬆	DICOM_VIP	10.224.94.10	2104	0	TCP	Layer 7	Proxy
⬆	DMWL_VIP	10.224.94.12	3320	0	TCP	Layer 7	Proxy
⬆	PORTAL_VIP	10.224.94.14	80	0	HTTP	Layer 7	Proxy
⬆	CHAT	-	-	0	HTTP	Layer 7	Proxy
⬆	PORTAL_VIP_STAND..	10.224.94.16	80	0	HTTP	Layer 7	Proxy
⬆	CHAT_STANDBY	-	-	0	HTTP	Layer 7	Proxy
⬆	CLIENT_VIP	10.224.94.18	80,443,21..	0	TCP	Layer 7	Proxy
⬆	CLIENT_DB_VIP	10.224.94.20	1521	0	TCP	Layer 7	Proxy
⬆	HL7_VIP	10.224.94.22	4001,4003..	0	TCP	Layer 7	Proxy

If one of the servers within a cluster fails its health check, that server will be colored red and the cluster will be colored yellow as shown below:



⚠	PORTAL_VIP	10.224.94.14	80	0	HTTP	Layer 7	Proxy
	REAL SERVER	IP	PORTS	WEIGHT	CONNS		
⬆	Portal1	10.224.94.110	443	100	0	Drain	Halt
⬆	Portal2	10.224.94.111	443	100	0	Drain	Halt
⬇	Portal3	10.224.94.112	443	100	0	Drain	Halt

If the services are up (green) verify that clients can connect to the VIPs and access all services.

> **Note** Make sure that DNS points at the VIPs rather than individual servers.

Once you have completed the verification process, continue to the next section and add a Secondary appliance to form the HA (active/passive) clustered pair.

12. 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 fully configured first, then the Secondary appliance can be added to create an HA pair. Once the HA pair is configured, load balanced services must be configured and modified on the Primary appliance. The Secondary appliance will be automatically kept in sync.

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.

12.1. 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:

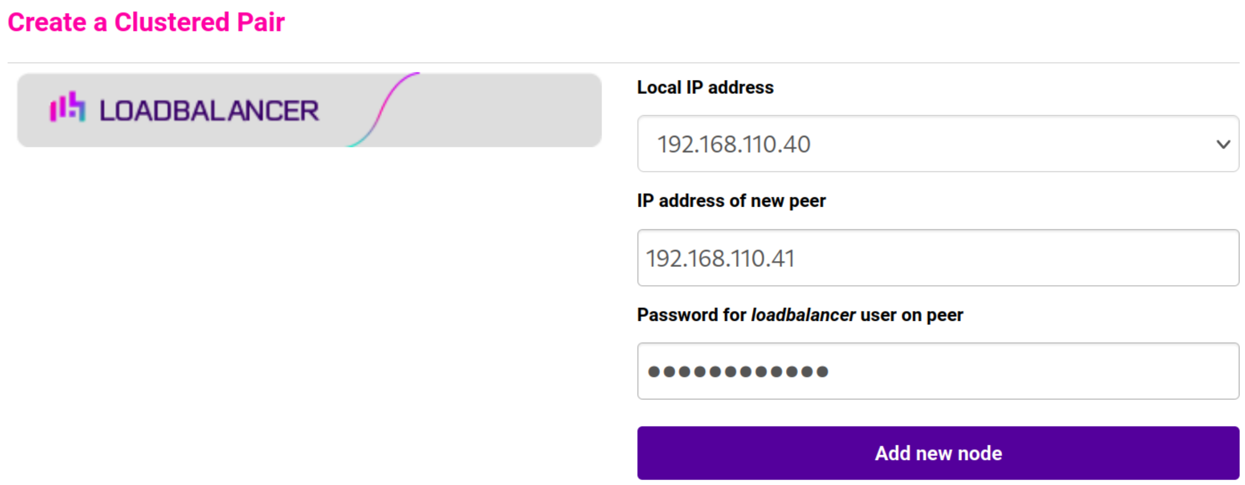
WebUI Main Menu Option	Sub Menu Option	Description
Local Configuration	Hostname & DNS	Hostname and DNS settings
Local Configuration	Network Interface Configuration	Interface IP addresses, bonding configuration and VLANs
Local Configuration	Routing	Default gateways and static routes
Local Configuration	System Date & time	Time and date related settings
Local Configuration	Physical – Advanced Configuration	Various appliance settings
Local Configuration	Portal Management	Portal management settings
Local Configuration	Security	Security settings
Local Configuration	SNMP Configuration	SNMP settings
Local Configuration	Graphing	Graphing settings
Local Configuration	License Key	Appliance licensing
Maintenance	Backup & Restore	Local XML backups
Maintenance	Software Updates	Appliance software updates
Maintenance	Fallback Page	Fallback page configuration
Maintenance	Firewall Script	Firewall (iptables) configuration
Maintenance	Firewall Lockdown Wizard	Appliance management lockdown settings

> **Important** Make sure that where any of the above have been configured on the Primary appliance, they're also configured on the Secondary.

12.2. Configuring the 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

Local IP address

192.168.110.40

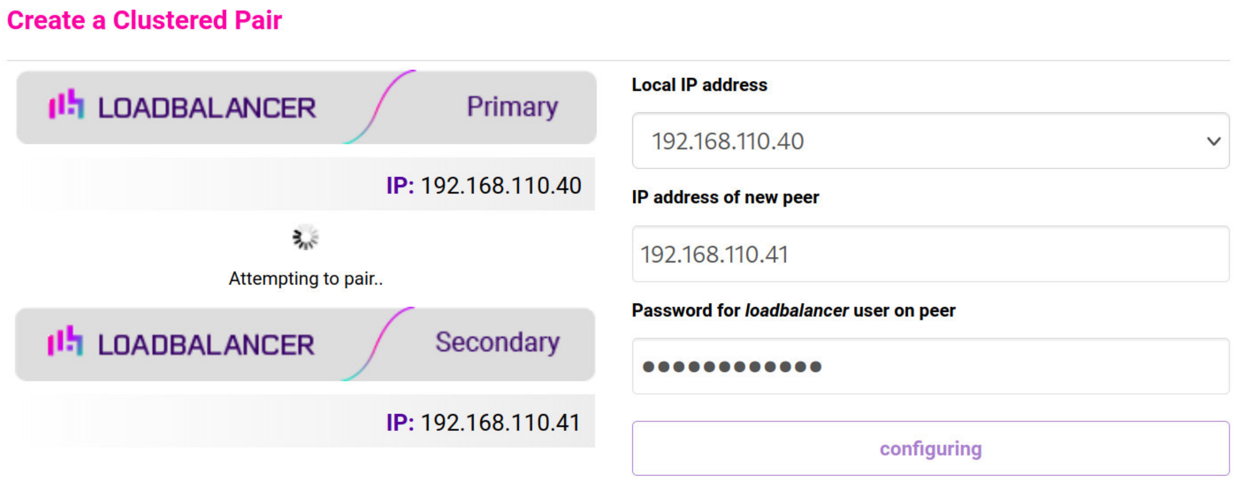
IP address of new peer

192.168.110.41

Password for *loadbalancer* user on peer

●●●●●●●●●●●●

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

IP: 192.168.110.40

Attempting to pair..

IP: 192.168.110.41

Local IP address

192.168.110.40

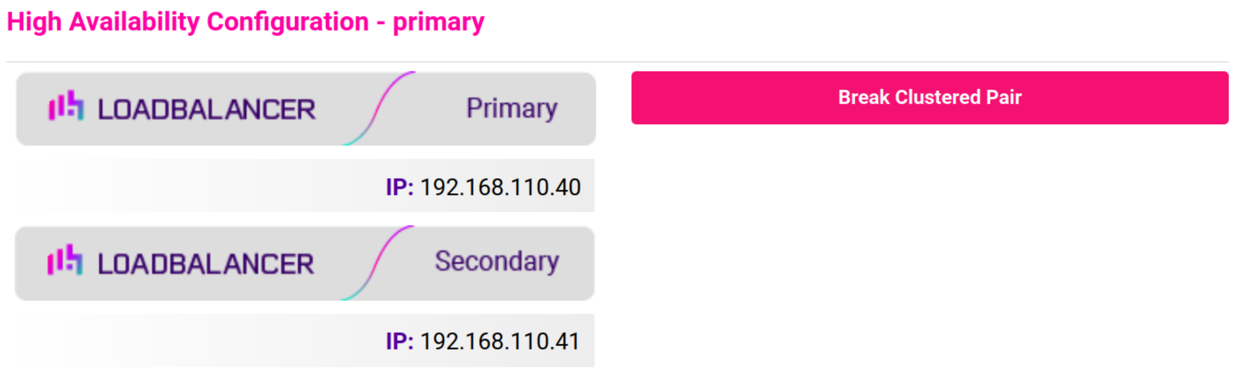
IP address of new peer

192.168.110.41

Password for *loadbalancer* user on peer

●●●●●●●●●●●●

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



High Availability Configuration - primary

IP: 192.168.110.40

IP: 192.168.110.41

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.

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

ℹ Note	For more details on configuring HA with 2 appliances, please refer to Appliance Clustering for HA.

ℹ Note	For details on testing and verifying HA, please refer to Clustered Pair Diagnostics.

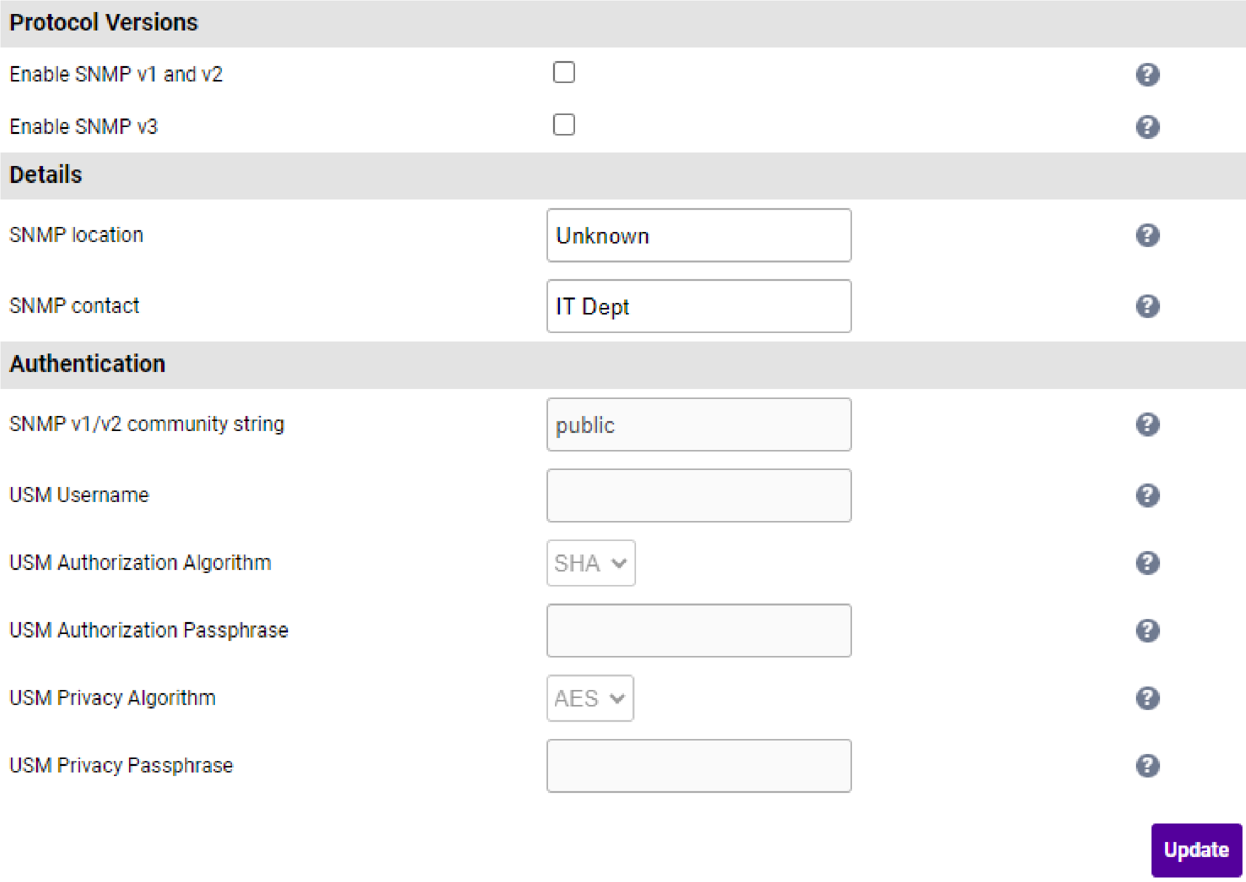
13. Optional Appliance Configuration

13.1. SNMP Configuration

The appliance supports SNMP v1, v2 and v3.

To configure SNMP:

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



Protocol Versions		
Enable SNMP v1 and v2	□	?
Enable SNMP v3	□	?
Details		
SNMP location	Unknown	?
SNMP contact	IT Dept	?
Authentication		
SNMP v1/v2 community string	public	?
USM Username		?
USM Authorization Algorithm	SHA	?
USM Authorization Passphrase		?
USM Privacy Algorithm	AES	?
USM Privacy Passphrase		?

2. Enable the required SNMP version(s).
3. Enter the required ***SNMP location*** and ***SNMP contact***.
4. For SNMP v1 & v2:

- Enter the required *SNMP v1/v2 community string*.

5. For SNMP v3:

   - Specify the *USM Username*.
   - Select the required *USM Authorization Algorithm*.
   - Specify the *USM Authorization Passphrase*, it should be at least 8 characters.
   - Select the required *USM Privacy Algorithm*.
   - Specify *USM Privacy Passphrase*, it should be at least 8 characters.

6. Click **Update**.

7. Restart SNMPD using the **Restart SNMPD** button at the top of the screen.

> Note
>
> Valid characters for the *Community string*, *USM Username*, *USM Authorization Passphrase* and *USM Privacy Passphrase* fields are: **a-z A-Z 0-9 [ ] # ~ _ * ! = - $ % ? { } @ : ; ^**

> Note
>
> For more information about the various OIDs and associated MIBs supported by the appliance, please refer to SNMP Reporting.

> Note
>
> If you need to change the port, IP address or protocol that SNMP listens on, please refer to Service Socket Addresses.

13.2. Configuring Email Alerts for Virtual Services

Email alerts can be configured for layer 4 and layer 7 Virtual Services. This enables emails to be sent when one or more of the associated Real Servers fail their health check and also when they subsequently start to pass their health check.

13.2.1. Layer 4

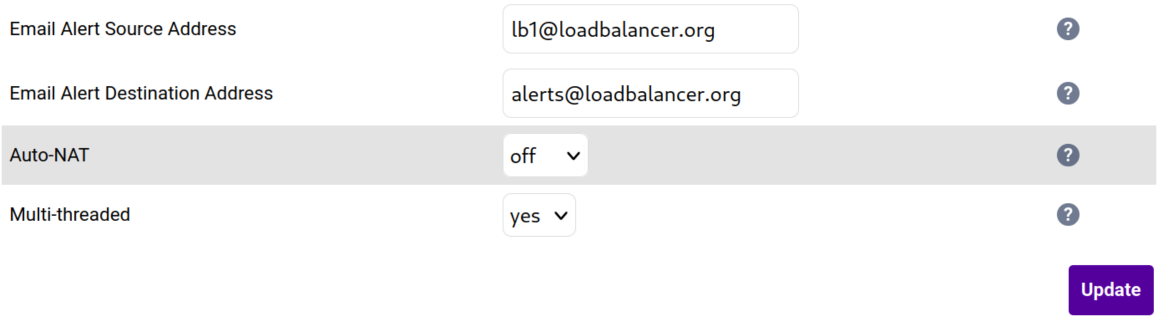
For layer 4 Virtual Services, settings can be configured globally for all VIPs or individually per VIP.

13.2.1.1. Global Layer 4 Email Settings

Once configured, these settings apply to all layer 4 VIPs by default.

To configure global email alert settings for layer 4 services:

1. Using the WebUI, navigate to: *Cluster Configuration > Layer 4 Advanced Configuration*.



Email Alert Source Address	lb1@loadbalancer.org
Email Alert Destination Address	alerts@loadbalancer.org
Auto-NAT	off
Multi-threaded	yes

2. Enter an appropriate email address in the *Email Alert Source Address* field.

```
e.g. lb1@loadbalancer.org
```

3. Enter an appropriate email address in the *Email Alert Destination Address* field.

```
e.g. alerts@loadbalancer.org
```

4. Click **Update**.

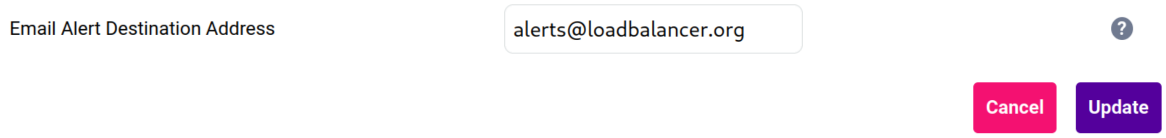
13.2.1.2. VIP Level Settings

> Note   VIP level settings override the global settings.

Once configured, these settings apply to the individual VIP.

To configure VIP level email alerts:

1. Using the WebUI, navigate to: *Cluster Configuration > Layer 4 Virtual Service* and click **Modify** next to the VIP to be configured.
2. Scroll down to the *Fallback Server* section.



Email Alert Destination Address	alerts@loadbalancer.org

3. Enter an appropriate email address in the *Email Alert Destination Address* field.

```
e.g. alerts@loadbalancer.org
```

4. Click **Update**.

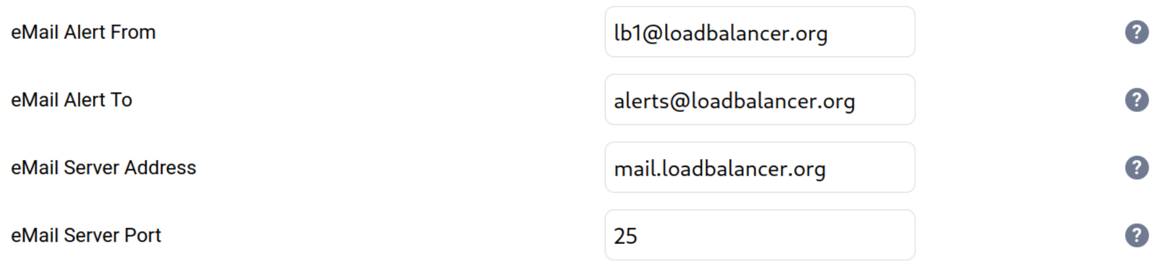
> Note   You can set the *Email Alert Source Address* field as explained above if required to configure a default source address.

13.2.2. Layer 7

For layer 7 services, email settings are configured globally for all VIPs.

To configure global email alert settings for layer 7 services:

1. Using the WebUI, navigate to: *Cluster Configuration > Layer 7 Advanced Configuration*.



eMail Alert From	lb1@loadbalancer.org
eMail Alert To	alerts@loadbalancer.org
eMail Server Address	mail.loadbalancer.org
eMail Server Port	25

2. Enter an appropriate email address in the ***eMail Alert From*** field.

```
e.g. lb1@loadbalancer.org
```

3. Enter an appropriate email address in the ***eMail Alert To*** field.

```
e.g. alerts@loadbalancer.org
```

4. Enter an appropriate IP address/FQDN in the ***eMail Server Address*** field.

```
e.g. mail.loadbalancer.org
```

5. Enter an appropriate port in the ***eMail Server Port*** field.

```
e.g. 25
```

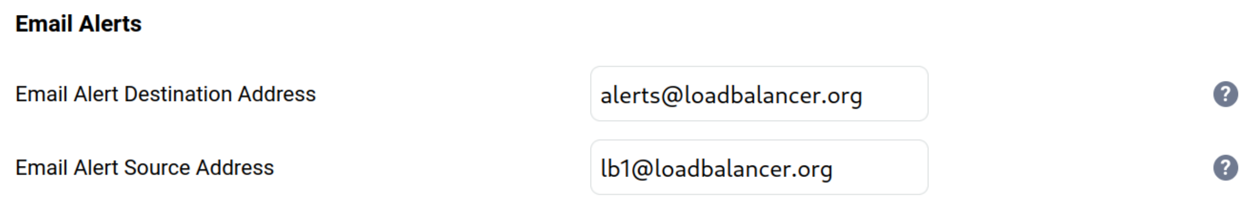
6. Click **Update**.

13.3. Configuring Email Alerts for Heartbeat

Email alerts can be setup for heartbeat once a clustered pair has been configured. This enables alerts to be sent when the primary/secondary communication state has changed. This can occur when the secondary appliance takes over from the primary, when the primary takes over from the secondary and also when there is a communication issue between the 2 appliances.

To configure email alert settings for Heartbeat:

1. Using the WebUI, navigate to: *Cluster Configuration > Heartbeat Configuration*.
2. Scroll down to the **Email Alerts** section.



Email Alerts

Email Alert Destination Address	alerts@loadbalancer.org
Email Alert Source Address	lb1@loadbalancer.org

3. Enter an appropriate email address in the *Email Alert Destination Address* field.
4. Enter an appropriate email address in the *Email Alert Source Address* field.
5. Click **Modify Heartbeat Configuration**.

13.4. Configuring a Smart Host (SMTP relay)

For Heartbeat (and layer 4 services), email alerts are sent from the load balancer directly to the mail server defined in the destination domain’s DNS MX record by default. Alternatively, a custom smart host (mail relay server) can be specified. A smart host is an email server through which approved devices can send emails. Where possible, we recommend that you use a smart host for email alerts as this often helps improve the deliverability of emails.

To configure a Smart Host:

1. Using the WebUI, navigate to: *Local Configuration > Physical - Advanced Configuration*.
2. Scroll down to the *SMTP Relay* section.
3. Specify the FQDN or IP address of the *Smart Host*.
4. Click **Update**.

> Note
>
> By default the *Smart Host* is set as the destination email domain’s DNS MX record when the *Email Alert Destination Address* is configured. It must either be left at its default setting or a custom smart host must be configured to enable email alerts to be sent.

14. Technical Support

If you require any assistance please contact support@loadbalancer.org.

15. Further Documentation

For additional information, please refer to the Administration Manual.

16. Appendix

16.1. Configuring VLAN Interfaces

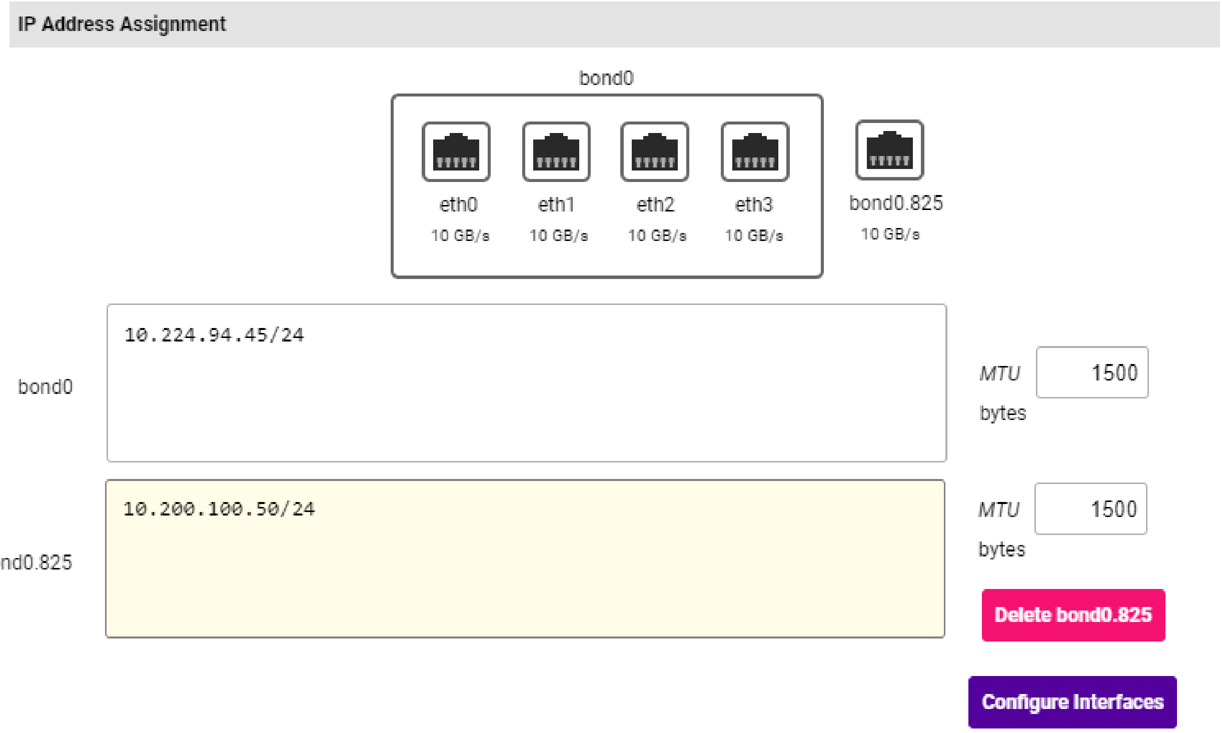
If the deployment requires the load balancer to be connected to multiple tagged VLANs, these must be configured on the appliance and an IP address must be set for each.

To configure a VLAN:

1. Using the appliance WebUI navigate to: *Local Configuration > Network Interface Configuration*.
2. Scroll down to the **VLAN** section.
3. Select the appropriate network adapter in the *Interface* dropdown.

> Note
>
> If you have run through the network configuration wizard and have not configured any additional network adapters then **eth0** should be selected.

4. Enter the appropriate *VLAN ID*, e.g. **825**.
5. Enter an appropriate IP address for the appliance within the VLAN, e.g. **10.200.100.50/24**.



IP Address Assignment

bond0: 10.224.94.45/24 — MTU 1500 bytes

bond0.825: 10.200.100.50/24 — MTU 1500 bytes

6. Click **Add VLAN**.
7. If required, repeat these steps to configure additional VLAN interfaces.

16.2. Configuring the Default Gateway

The default gateway is configured during the network setup wizard. If this needs to be changed follow the steps below.

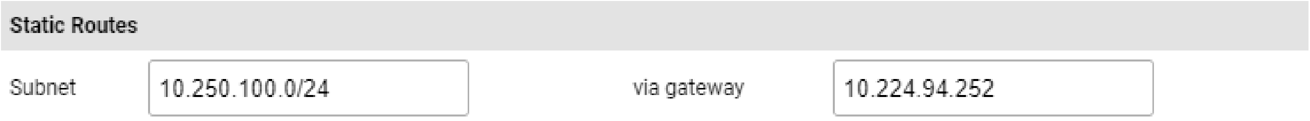
1. Using the appliance WebUI navigate to: *Local Configuration > Routing*.
2. Set the required gateway address.
3. Click **Configure Routing**.

16.3. Traffic Routing Options

The load balancer enables static routes and Policy Based Routing (PBR) to be configured. Static routes can be used where it makes sense for the rule to be based on the destination, PBR can be used when it makes sense for the rule to be based on the source.

16.3.1. Configuring Static Routes

Using the WebUI menu option: *Local Configuration > Routing* the following static route could be added to the load balancer:



Static Routes

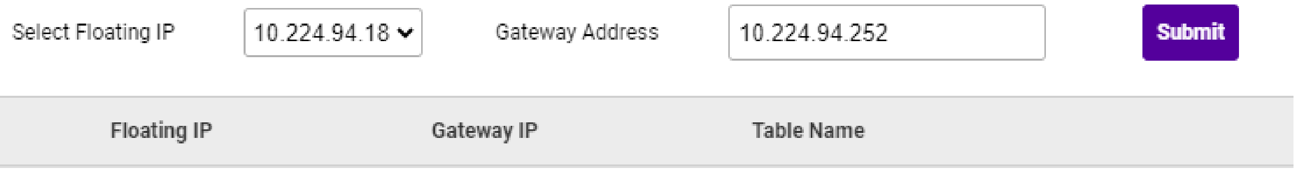
Subnet: 10.250.100.0/24

via gateway: 10.224.94.252

This would force return traffic destined for the 10.250.100.0/24 network to be sent via the 10.224.94.252 gateway.

16.3.2. Configuring PBR (Policy Based Routing)

Using the WebUI menu option: *Cluster Configuration > PBR Default Gateways* the following gateway could be added to the load balancer:



Select Floating IP: 10.224.94.18

Gateway Address: 10.224.94.252

Floating IP	Gateway IP	Table Name

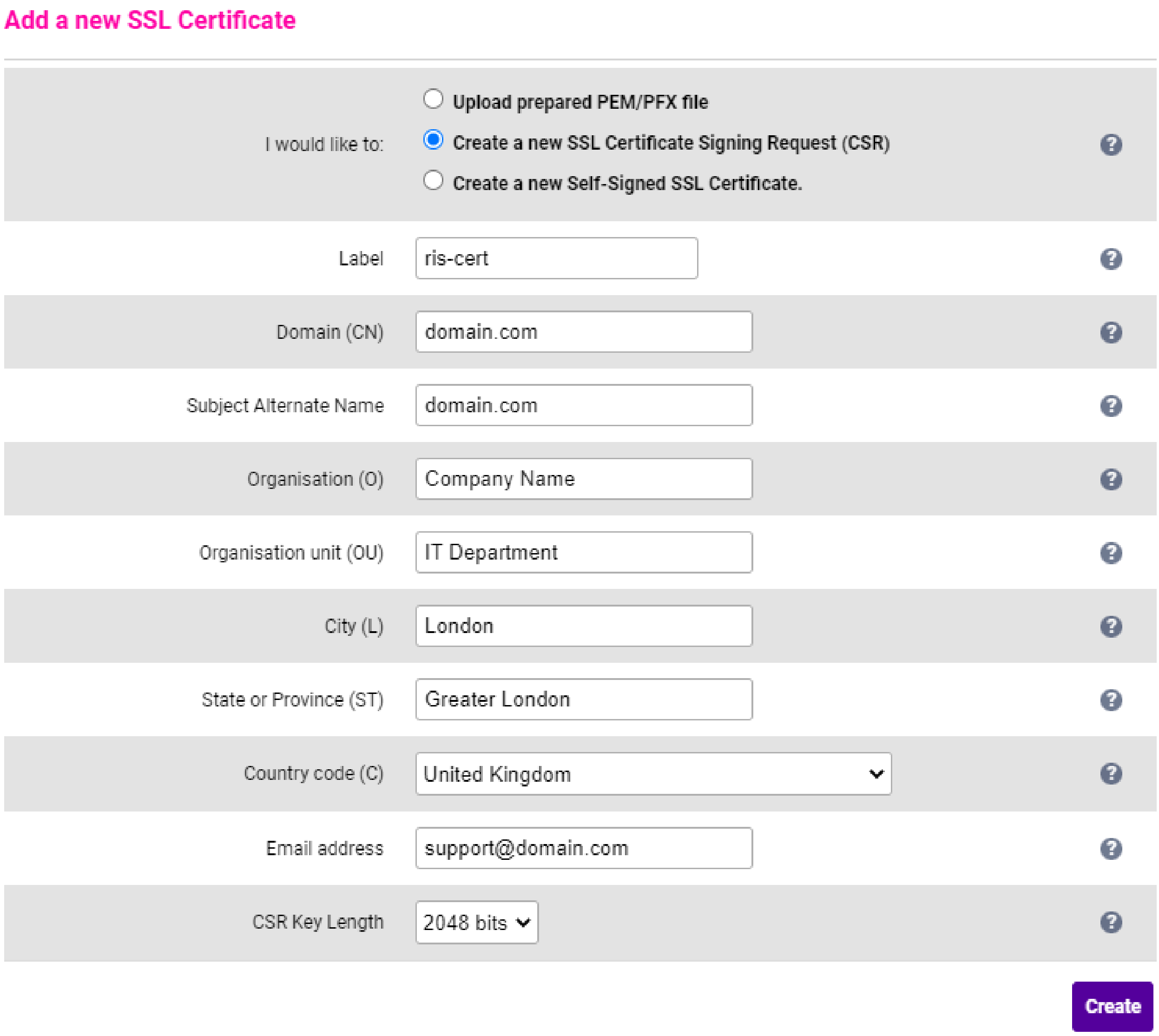
This would ensure that all traffic with a source address of 10.224.94.18 is sent via the 10.224.94.252 gateway.

16.4. Generating a CSR on the Load Balancer

If you have an SSL certificate in either PFX or PEM file format, this can be uploaded to the Load balancer using the certificate upload option. Alternatively, you can create a Certificate Signing Request (CSR) on the load balancer and send this to your chosen CA to create a new certificate.

To generate a CSR:

1. Using the WebUI, navigate to: *Cluster Configuration > SSL Certificates*.
2. Click **Add a new SSL Certificate** & select *Create a New SSL Certificate (CSR)*.



Add a new SSL Certificate

I would like to:	○ Upload prepared PEM/PFX file ● Create a new SSL Certificate Signing Request (CSR) ○ Create a new Self-Signed SSL Certificate.
Label	ris-cert
Domain (CN)	domain.com
Subject Alternate Name	domain.com
Organisation (O)	Company Name
Organisation unit (OU)	IT Department
City (L)	London
State or Province (ST)	Greater London
Country code (C)	United Kingdom
Email address	support@domain.com
CSR Key Length	2048 bits

3. Enter a suitable ***Label*** (name) for the certificate.
4. Populate the remaining fields according to your requirements.

> **Note** To specify multiple SANs, separate each name with a comma.

5. Once all fields are complete click **Create**.
6. To view the CSR click **Modify** next to the new certificate, then expand the Certificate Signing Request (CSR) section.
7. Copy the CSR and send this to your chosen CA.
8. Once received, copy/paste your signed certificate into the ***Your Certificate*** section.
9. Intermediate and root certificates can be copied/pasted into the ***Intermediate Certificate*** and ***Root Certificate*** sections as required.
10. Click **Update** to complete the process.

The new certificate will now be displayed under ***Cluster Configuration > SSL Certificates***.

17. Document Revision History

Version	Date	Change	Reason for Change	Changed By
1.0	22 March 2024	Initial version		RJC

LOADBALANCER

Visit us: www.loadbalancer.org

Phone us: +44 (0)330 380 1064

Phone us: +1 833 274 2566

Email us: info@loadbalancer.org

Follow us: @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.