LOADBALANCER

DEPLOYMENT GUIDE

Load Balancing Meditech RESTful API

Version 1.3.0

Table of Contents

1. About this Guide

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

For more information about initial appliance deployment, network configuration and using the Web User Interface (WebUI), please also refer to the Administration Manual.

2. Loadbalancer.org Appliances Supported

All our products can be used with Meditech API servers. For full specifications of available models please refer to https://www.loadbalancer.org/products/enterprise.

Some features may not be available or fully supported in all cloud platforms due to platform specific limitations. For more details, please refer to the "Main Differences to our Standard (Non-Cloud) Product" section in the appropriate cloud platform Quick Start Guide or check with Loadbalancer.org support.

3. Software Versions Supported

3.1. Loadbalancer.org Appliance

- V8.9.1 and later

> **Note** The screenshots used throughout this document aim to track the latest Loadbalancer.org software version. If you're using an older version, or the very latest, the screenshots presented here may not match your WebUI exactly.

3.2. Meditech RESTful API

- All versions

4. Meditech RESTful API

The RESTful API Infrastructure allows Meditech and third party vendor software to securely access the Meditech EHR through APIs. Interoperability Services (or IOPS) — which is a component of the RESTful API Infrastructure and installed on the same machine(s) — adds a set of APIs to meet Meaningful Use Stage 3 (MU3) and Imaging Appropriate Use Criteria (AUC) requirements. RESTful API is independent from any other web products or interoperability interfaces Meditech offers and requires dedicated hardware.

5. Load Balancing Meditech RESTful API

> **Note** It's highly recommended that you have a working Meditech API environment first before implementing the load balancer.

5.1. Load Balancing & HA Requirements

An optimal RESTful API Infrastructure configuration consists of two or more servers running the RESTful API services as well as Interoperability Services. The cluster helps to ensure better performance and failover protection for the Infrastructure. These servers host the web services which clients connect to.

As mentioned here, Meditech recommend either SSL termination or SSL bridging when using a load balancer. SSL passthrough where SSL is terminated on the backend API servers is not recommended.

Meditech also recommend that one VIP is used for all API environments and a separate VIP is used for all Application environments.

5.2. Option 1 - SSL Termination

Here, the connection to the appliance is encrypted, but the connection from the appliance to the RESTful services is not encrypted.

5.2.1. Virtual Service (VIP) Requirements

Ref.	VIP Name	Mode	Port(s)	Persistence Mode	Health Check
S1-VIP1	Meditech-API	L7 SNAT	80	None	HTTP (HEAD)
S1-VIP2	Meditech-APP	L7 SNAT	8081	None	HTTP (HEAD)

5.2.2. TLS/SSL Termination

SSL Termination is configured on the load balancer for both VIP1 and VIP2. This provides a corresponding HTTPS Virtual Service for these VIPs. Certificates in PEM or PFX format can be uploaded to the load balancer.

5.3. Option 2 - SSL Bridging

Here, the connection to the appliance is encrypted and the connection from the appliance to the API servers is also encrypted.

5.3.1. Virtual Service (VIP) Requirements

Ref.	VIP Name	Mode	Port(s)	Persistence Mode	Health Check
S2-VIP1	Meditech-API	L7 SNAT	80	None	HTTPS (HEAD)
S2-VIP2	Meditech-APP	L7 SNAT	8888	None	HTTPS (HEAD)

5.3.2. TLS/SSL Termination & Backend Re-encryption

As per option 1, SSL Termination is configured on the load balancer for VIP1 and VIP2. In addition, backend re-encryption is also enabled for both VIPs. This forces the connections from the appliance to the backend (Real) servers to be encrypted.

> **Note** Each Meditech API server must be configured for HTTPS and have appropriate SSL/TLS certificates installed.

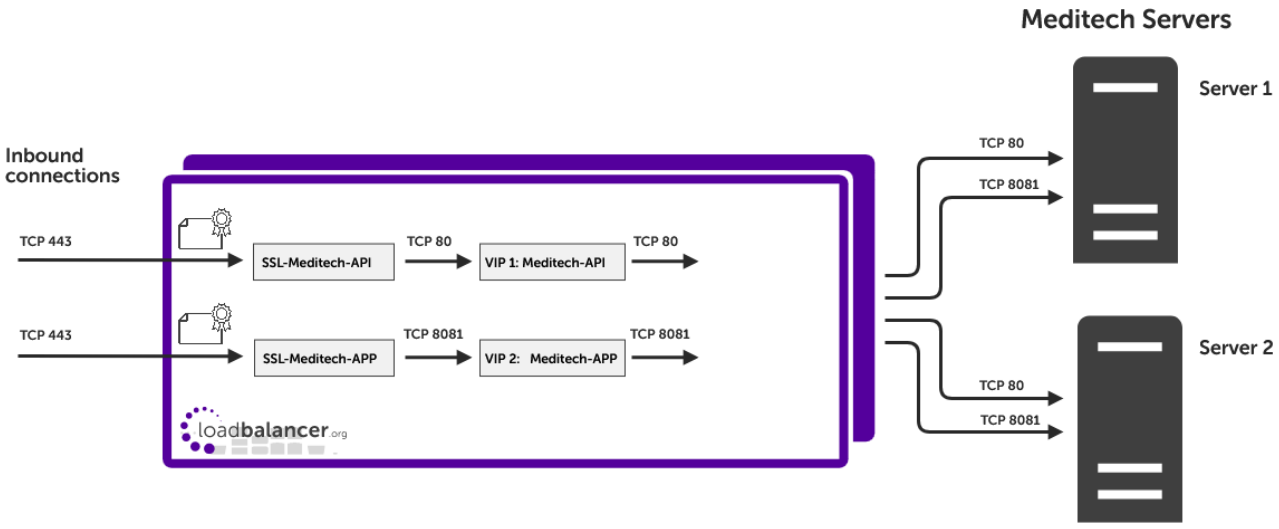
6. Deployment Concept

Once the load balancer is deployed, clients connect to the Virtual Services (VIPs) rather than connecting directly to one of the Meditech API servers. These connections are then load balanced across the Meditech servers to distribute the load according to the load balancing algorithm selected.

> **Note** The load balancer can be deployed as a single unit, although Loadbalancer.org recommends a clustered pair for resilience & high availability. Please refer to the section Configuring HA - Adding a Secondary Appliance in the appendix for more details on configuring a clustered pair.

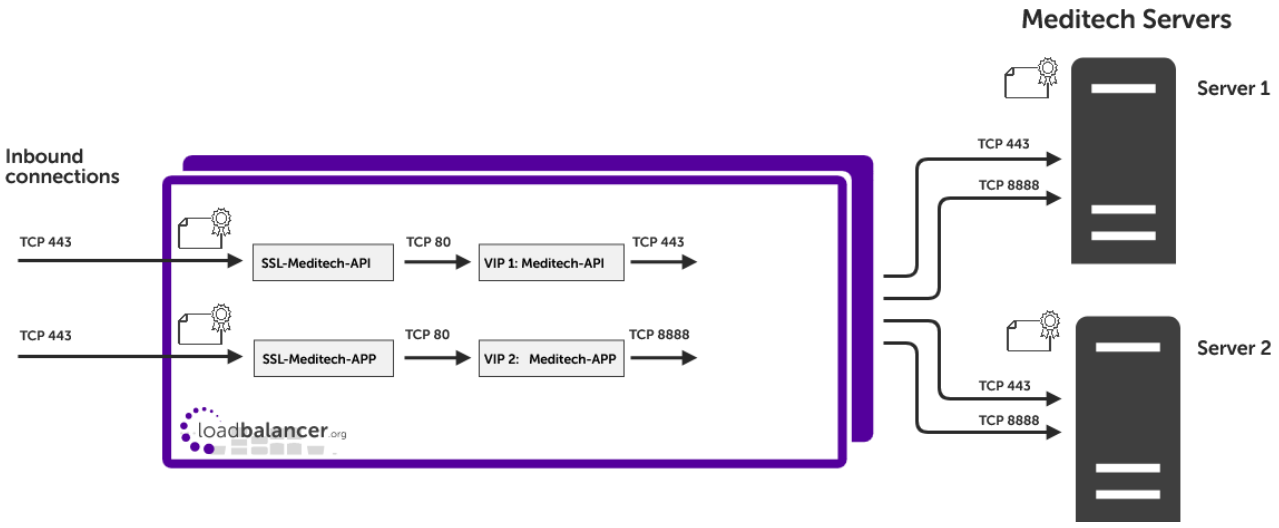
6.1. Option 1 - SSL Termination

Here, data is encrypted from the client to the load balancer, but is unencrypted from the load balancer to the backend servers. Certificates must be installed on the load balancer.



6.2. Option 2 - SSL Bridging

Here, data is encrypted from the client to the load balancer and is also encrypted from the load balancer to the backend servers. Certificates must be installed on the load balancer and on the Meditech servers.



7. Load Balancer Deployment Methods

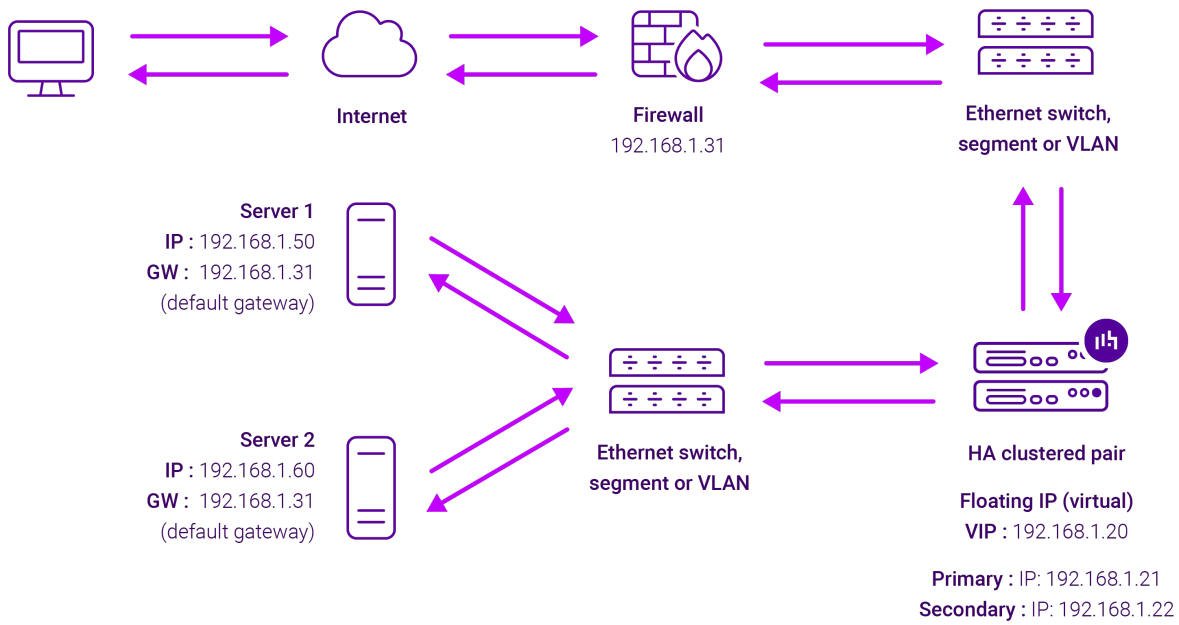
The load balancer can be deployed in 4 fundamental ways: ***Layer 4 DR mode***, ***Layer 4 NAT mode***, ***Layer 4 SNAT mode,*** and ***Layer 7 SNAT mode***.

For Meditech RESTful API, using layer 7 SNAT mode is recommended due to it being a full proxy meaning the load balanced Real Servers do not need to be changed in any way.

layer 7 SNAT mode is described below and is 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. The image below shows an example network diagram for this mode.



- Because layer 7 SNAT mode is a full proxy, Real Servers in the cluster can be on any accessible network 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, **eth1** is typically used for client side connections and **eth0** is used for Real Server connections, although this is not mandatory since any interface can be used for any purpose.
- 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 Meditech RESTful API for Load Balancing

Some changes must be made to the Meditech RESTful API server environment in order for them to be correctly load balanced.

8.1. DNS Entries

A DNS entry is needed for the API and Application end-point for each MRI or HIM database (both TEST and LIVE). These records should all point to VIPs on your Load Balancer - you may use one or multiple VIPs when configuring your Load Balancer.

It is suggested that the API services use different VIP(s) from Application services. This makes it easier to restrict access to the Application to only those clients that are on your network. If they shared a VIP, your firewall would need to be able to do deep packet inspection and disallow access to the hostnames for the Application services when accessed over the Internet.

8.1.1. Example

If you have 3 LIVE rings with 1 HIM database each and 3 TEST rings with 1 HIM database each, we would expect the following DNS entries:

```
mtrestapis-live01.CUSTOMER-DOMAIN
mtrestapis-live02.CUSTOMER-DOMAIN
mtrestapis-live03.CUSTOMER-DOMAIN
mtrestapis-test01.CUSTOMER-DOMAIN
mtrestapis-test02.CUSTOMER-DOMAIN
mtrestapis-test03.CUSTOMER-DOMAIN
mtrestapps-live01.CUSTOMER-DOMAIN
mtrestapps-live02.CUSTOMER-DOMAIN
mtrestapps-live03.CUSTOMER-DOMAIN
mtrestapps-test01.CUSTOMER-DOMAIN
mtrestapps-test02.CUSTOMER-DOMAIN
mtrestapps-test03.CUSTOMER-DOMAIN
```

When not exposing the Application to the Internet, only the `mtrestapis-*` entries would resolve on your public DNS. The DNS entries allow the infrastructure to differentiate requests as it is possible that an identifier may be reused in one or more databases. Additionally, the API and Application services run on different ports and within different processes because the workloads are significantly different.

9. Loadbalancer.org Appliance – the Basics

9.1. 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.

9.2. Initial Network Configuration

After boot up, follow the instructions on the appliance console to configure the management IP address, subnet mask, default gateway, DNS servers and other network and administrative settings.

Important	Be sure to set a secure password for the load balancer, when prompted during the setup routine.

9.3. 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.

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

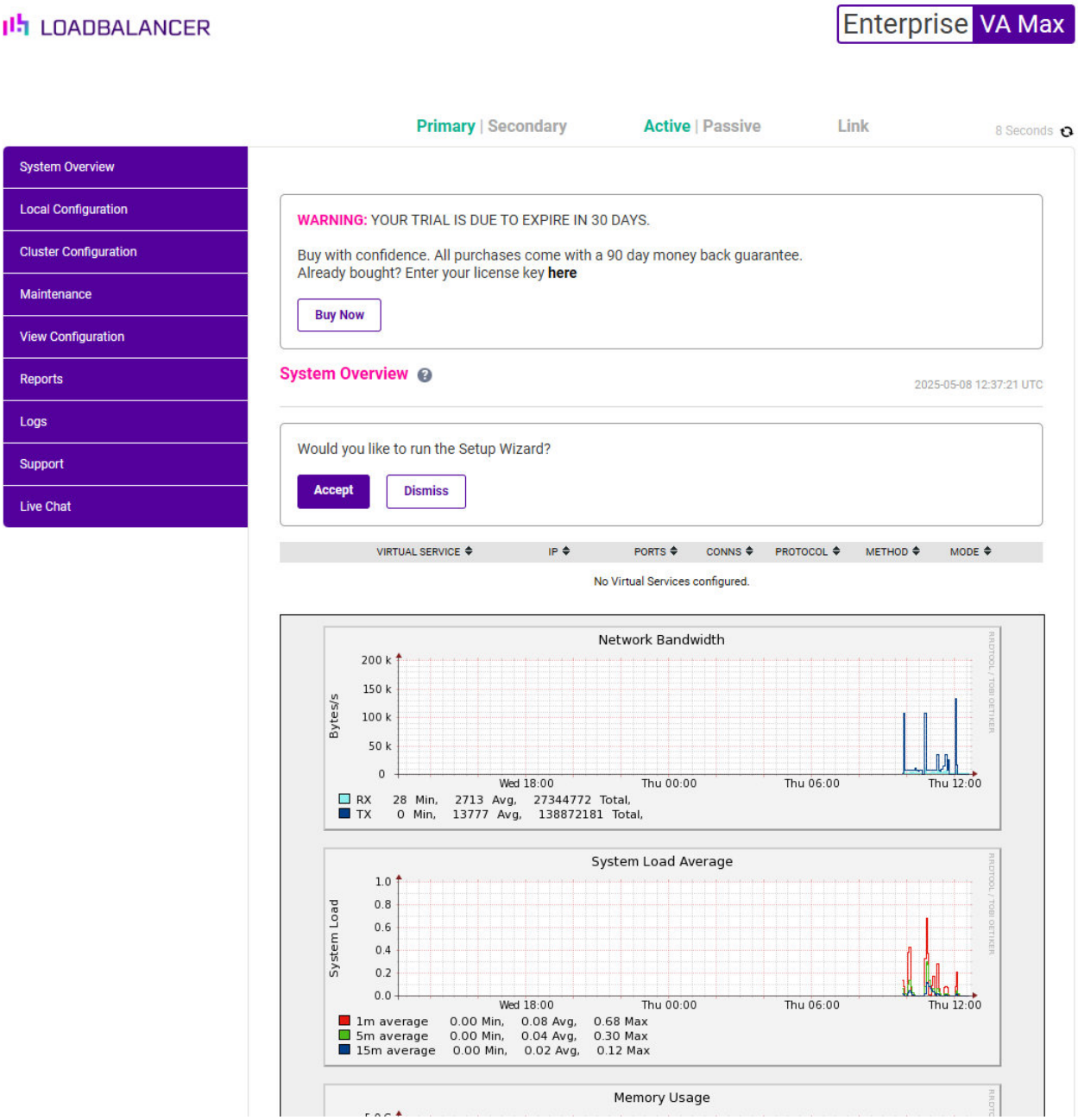
refer to Service Socket Addresses.

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:



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.

9.3.1. 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 creating 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

9.4. Appliance Software Update

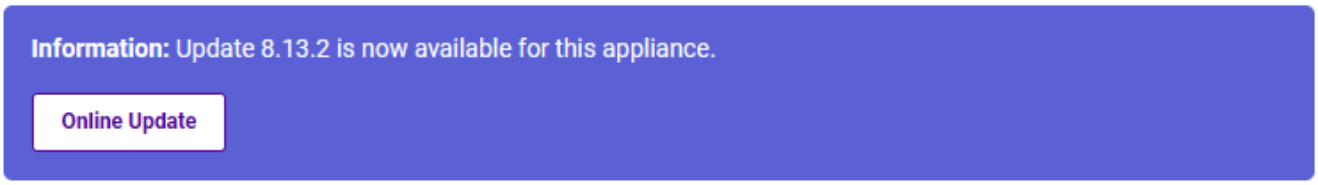
We recommend that the appliance is kept up to date to ensure that you benefit from the latest bug fixes, security updates and feature improvements. Both online and offline update are supported.

> **Note** For full details, please refer to Appliance Software Update in the Administration Manual.

> **Note** Services may need to be restarted/reloaded after the update process completes or in some cases a full appliance restart may be required. We therefore recommend performing the update during a maintenance window.

9.4.1. Online Update

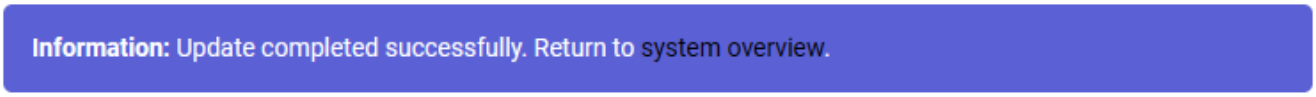
The appliance periodically contacts the Loadbalancer.org update server (**update.loadbalancer.org**) and checks for updates. This is the default behavior and can be disabled if preferred. If an update is found, a notification similar to the example below will be displayed at the top of the WebUI:



Click **Online Update**. A summary of all new features, improvements, bug fixes and security updates included in the update will be displayed. Click **Update** at the bottom of the page to start the update process.

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

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



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

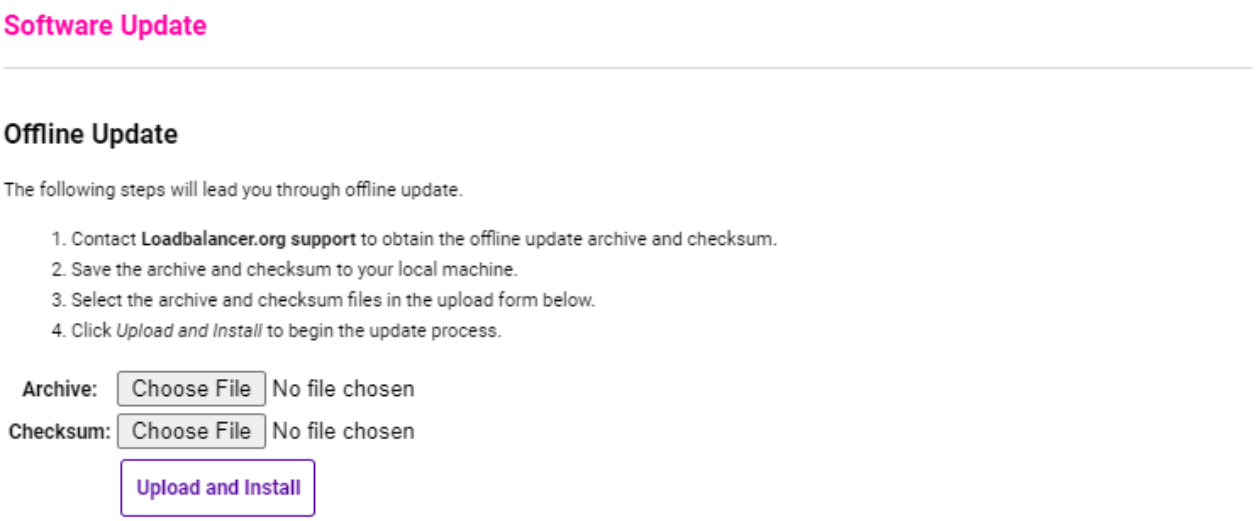
9.4.2. Offline Update

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

To check for the latest version, please refer to our product roadmap page available here. To obtain the latest offline update files contact support@loadbalancer.org.

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:



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.

9.5. 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

Protocol	Port	Purpose
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.

9.6. HA Clustered Pair Configuration

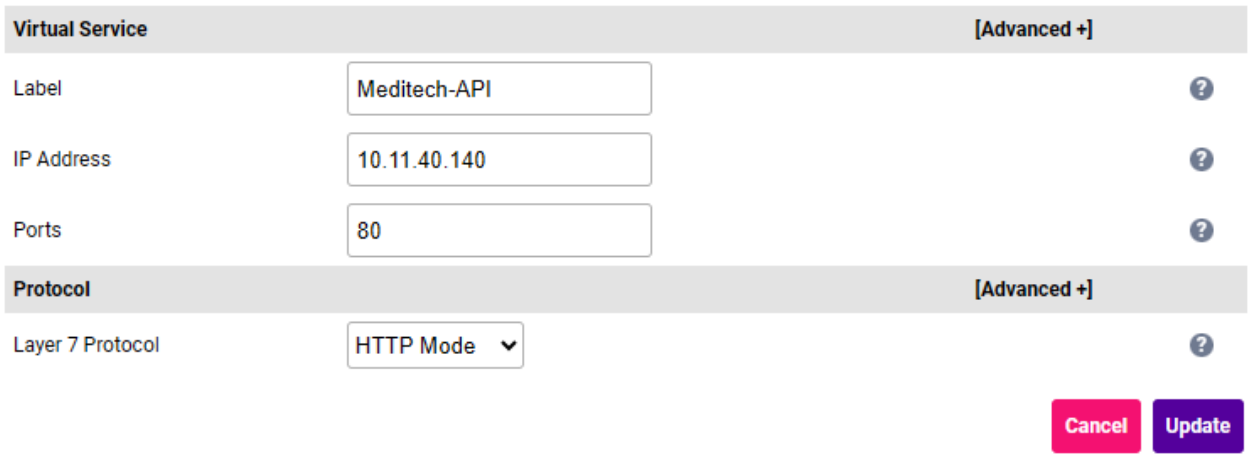
Loadbalancer.org recommend that load balancer appliances are deployed in pairs for high availability. In this guide a single unit is deployed first, adding a secondary unit is covered in Configuring HA - Adding a Secondary Appliance.

10. Appliance Configuration for Meditech API : Option 1 - SSL Termination

10.1. S1-VIP1 - Meditech-API

10.1.1. Virtual Service (VIP) Configuration

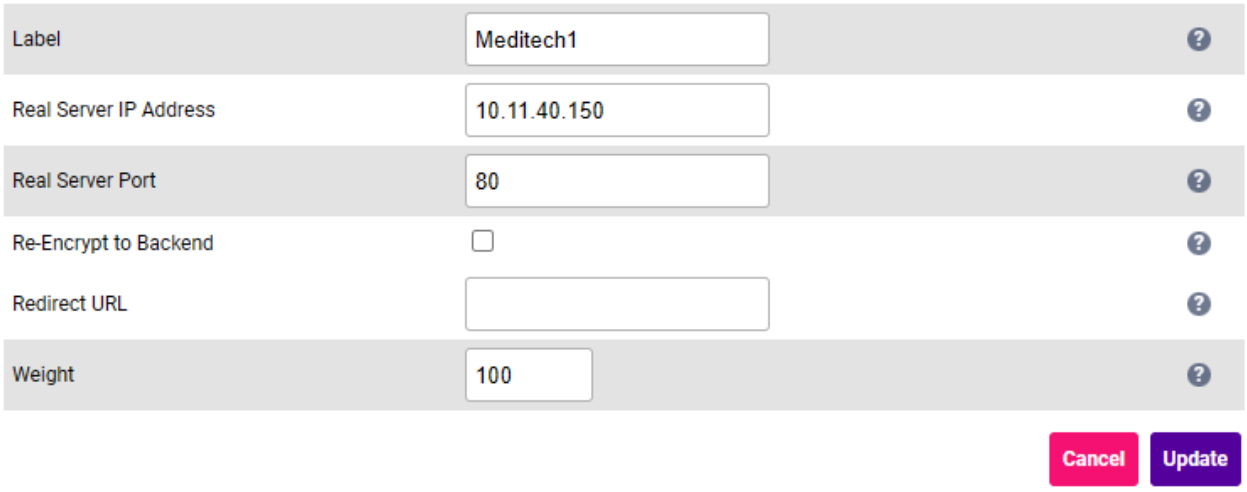
1. Using the WebUI, navigate to *Cluster Configuration > Layer 7 – Virtual Services* and click on **Add a new Virtual Service**.
2. Enter the following details:



3. Define the *Label* for the Virtual Service as required, e.g. **Meditech-API**.
4. Set the *Virtual Service IP Address* field to the required IP address, e.g. **10.11.40.140**.
5. Set the *Ports* field to **80**.
6. Set the *Layer 7 Protocol* to **HTTP Mode**.
7. Click **Update** to create the Virtual Service.
8. Now click **Modify** next to the newly created VIP.
9. Scroll to the *Persistence* section.
    - Set the *Persistence Mode* to **None**.
10. Scroll to the *Health Checks* section.
    - Set the *Health Checks* to **Negotiate HTTP (HEAD)**.
11. Scroll to the *Other* section and click **[Advanced]**.
    - Set *Force to HTTPS* to **Yes**.
12. Leave all other settings at their default value.
13. Click **Update**.

10.1.2. Define the Associated Real Servers (RIPs)

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



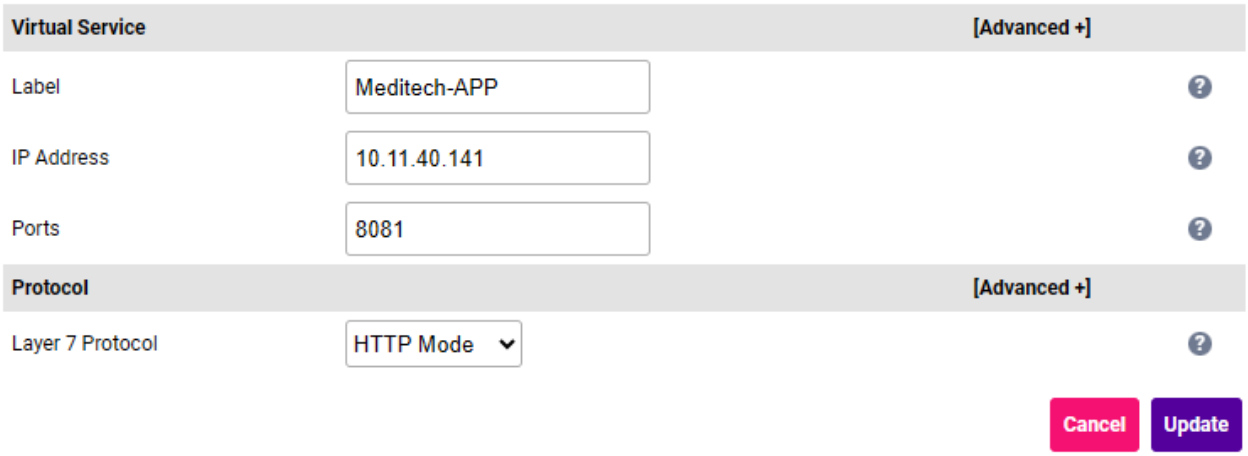
3. Define the *Label* for the Real Server as required, e.g. **Meditech1**.
4. Set the *Real Server IP Address* field to the required IP address, e.g. **10.11.40.150**.
5. Set the *Real Server Port* field to **80**.
6. Leave all other settings at their default value.
7. Click **Update**.

8. Repeat these steps to add the remaining Meditech server(s).

10.2. S1-VIP2 - Meditech-APP

10.2.1. Virtual Service (VIP) Configuration

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

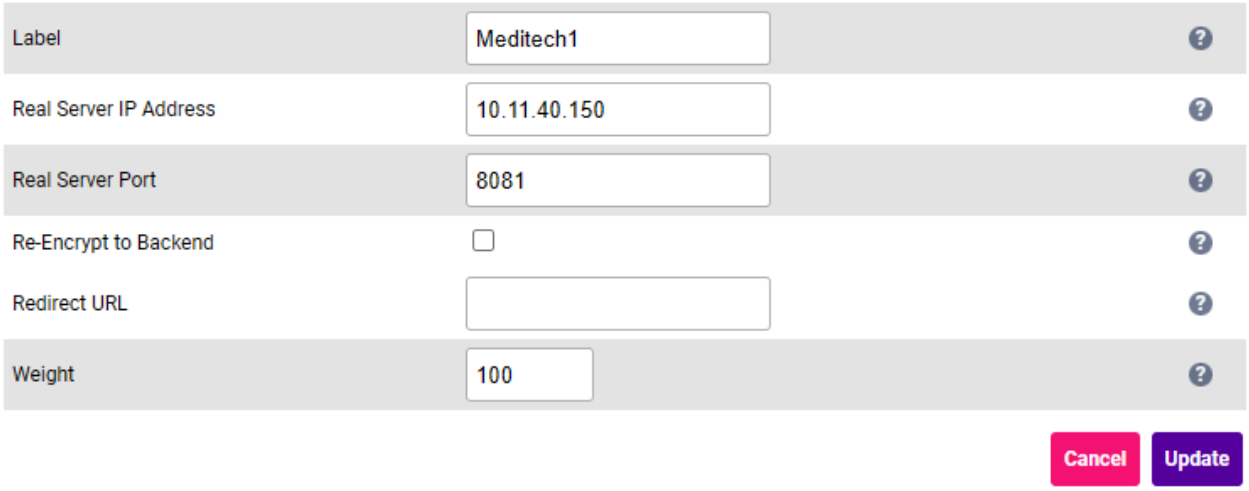


3. Define the *Label* for the Virtual Service as required, e.g. **Meditech-APP**.
4. Set the *Virtual Service IP Address* field to the required IP address, e.g. **10.11.40.141**.
5. Set the *Ports* field to **8081**.
6. Set the *Layer 7 Protocol* to **HTTP Mode**.
7. Click **Update** to create the Virtual Service.
8. Now click **Modify** next to the newly created VIP.
9. Scroll to the *Persistence* section.
   - Set the *Persistence Mode* to **None**.
10. Scroll to the *Health Checks* section.
    - Set the *Health Checks* to **Negotiate HTTP (HEAD)**.
11. Scroll to the *Other* section and click **[Advanced]**.
    - Set *Force to HTTPS* to **Yes**.
12. Leave all other settings at their default value.
13. Click **Update**.

10.2.2. Define the Associated Real Servers (RIPs)

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

2. Enter the following details:



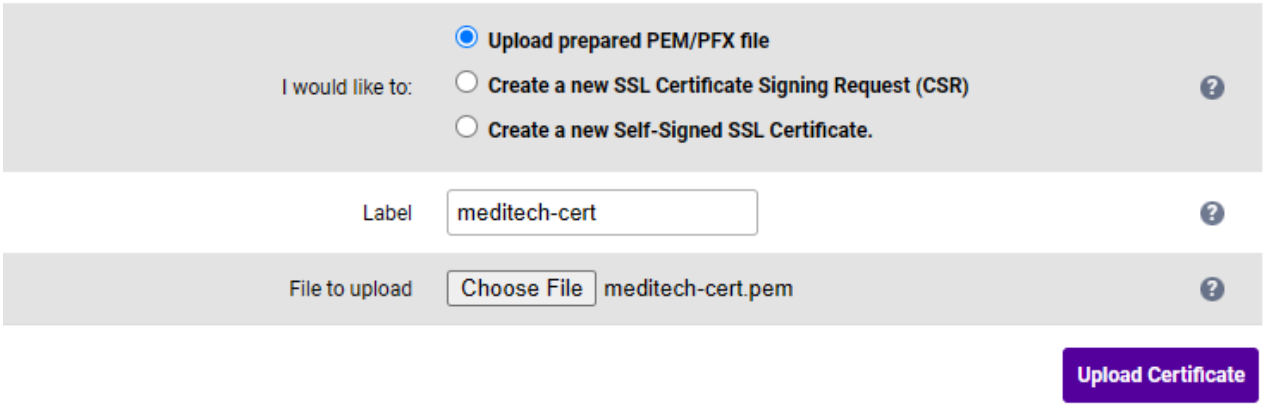
3. Define the *Label* for the Real Server as required, e.g. **Meditech1**.
4. Set the *Real Server IP Address* field to the required IP address, e.g. **10.11.40.150**.
5. Set the *Real Server Port* field to **8081**.
6. Leave all other settings at their default value.
7. Click **Update**.
8. Repeat these steps to add the remaining Meditech server(s).

10.3. Upload the SSL Certificate

Certificates in either PEM or PFX format can be uploaded.

> **Note** If the API and APP services use a different certificate, run through the steps below twice to upload both certs. Use a relevant label (name) for each certificate.

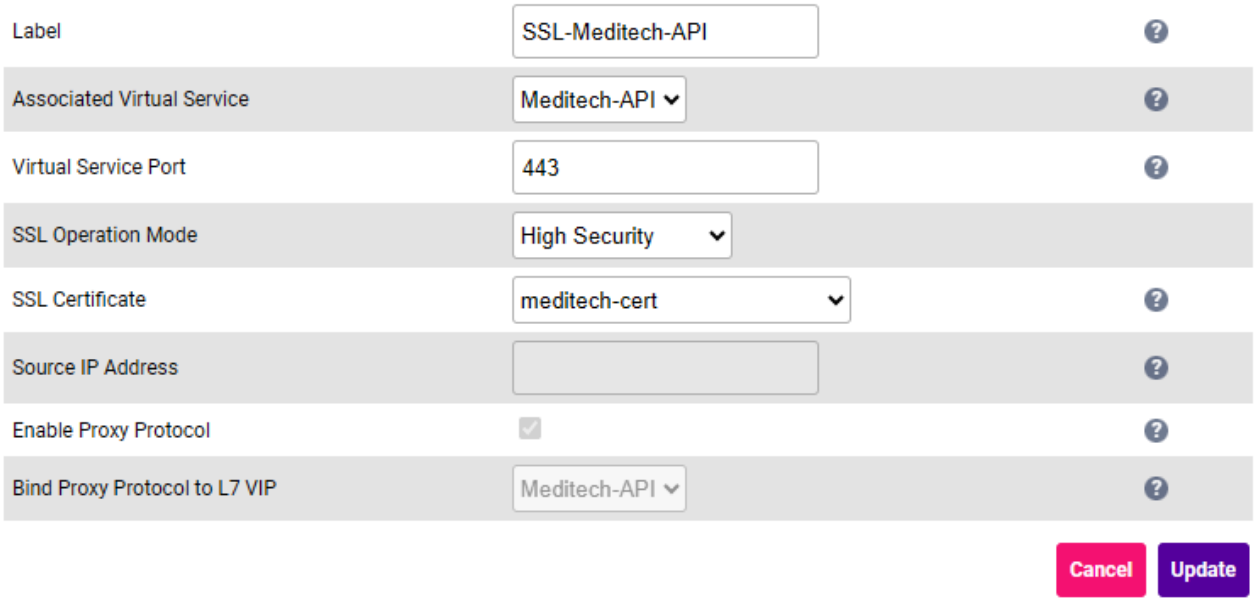
1. Using the WebUI, navigate to *Cluster Configuration > SSL Certificate* and click **Add a new SSL Certificate**.
2. Select the option **Upload prepared PEM/PFX file**.
3. Enter the following details:



4. Specify an appropriate *Label*, e.g. **meditech-cert**.
5. Click **Choose File**.
6. Browse to and select the relevant PEM or PFX file.
7. For PFX files specify the password if required.
8. Click **Upload Certificate**.

10.4. Configure SSL Termination

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



3. Using the *Associated Virtual Service* drop-down, select the Virtual Service created above, e.g. **Medtech-API**.

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

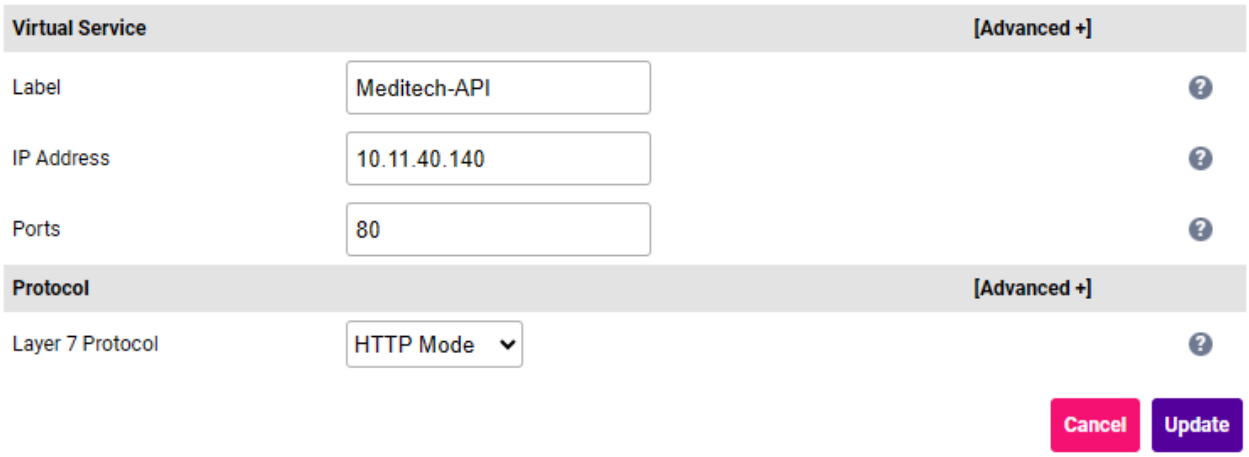
4. Ensure that the *Virtual Service Port* is set to **443**.
5. Leave *SSL Operation Mode* set to **High Security**.
6. Select the relevant *SSL Certificate* uploaded previously.
7. Leave all other settings at their default value.
8. Click **Update**.
9. Now repeat these steps to configure the SSL termination for the **Meditech-APP** VIP.

11. Appliance Configuration for Meditech API : Option 2 - SSL Bridging

11.1. S2-VIP1 - Meditech-API

11.1.1. Virtual Service (VIP) Configuration

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

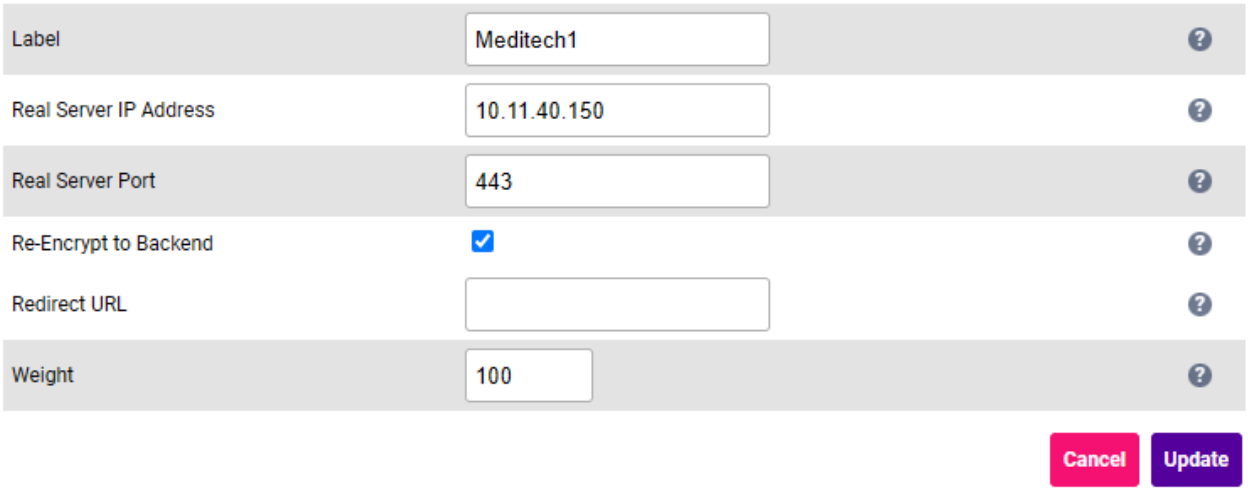


3. Define the *Label* for the Virtual Service as required, e.g. **Meditech-API**.
4. Set the *Virtual Service IP Address* field to the required IP address, e.g. **10.11.40.140**.
5. Set the *Ports* field to **80**.
6. Set the *Layer 7 Protocol* to **HTTP Mode**.
7. Click **Update** to create the Virtual Service.
8. Now click **Modify** next to the newly created VIP.
9. Scroll to the *Persistence* section.
   - Set the *Persistence Mode* to **None**.
10. Scroll to the *Health Checks* section.
    - Set the *Health Checks* to **Negotiate HTTPS (HEAD)**.
11. Scroll to the *SSL* section.
    - Enable (check) *Enable Backend Encryption*.
12. Scroll to the *Other* section and click **[Advanced]**.
    - Set *Force to HTTPS* to **Yes**.
13. Leave all other settings at their default value.

14. Click **Update**.

11.1.2. Define the Associated Real Servers (RIPs)

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

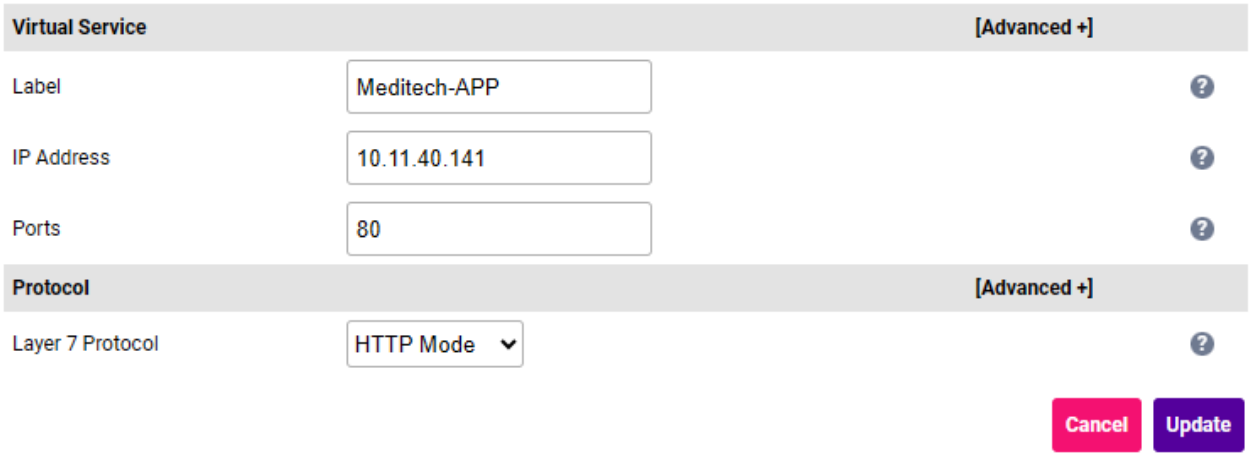


3. Define the *Label* for the Real Server as required, e.g. **Meditech1**.
4. Set the *Real Server IP Address* field to the required IP address, e.g. **10.11.40.150**.
5. Set the *Real Server Port* field to **443**.
6. Leave all other settings at their default value.
7. Click **Update**.
8. Repeat these steps to add the remaining Meditech server(s).

11.2. S2-VIP2 - Meditech-APP

11.2.1. Virtual Service (VIP) Configuration

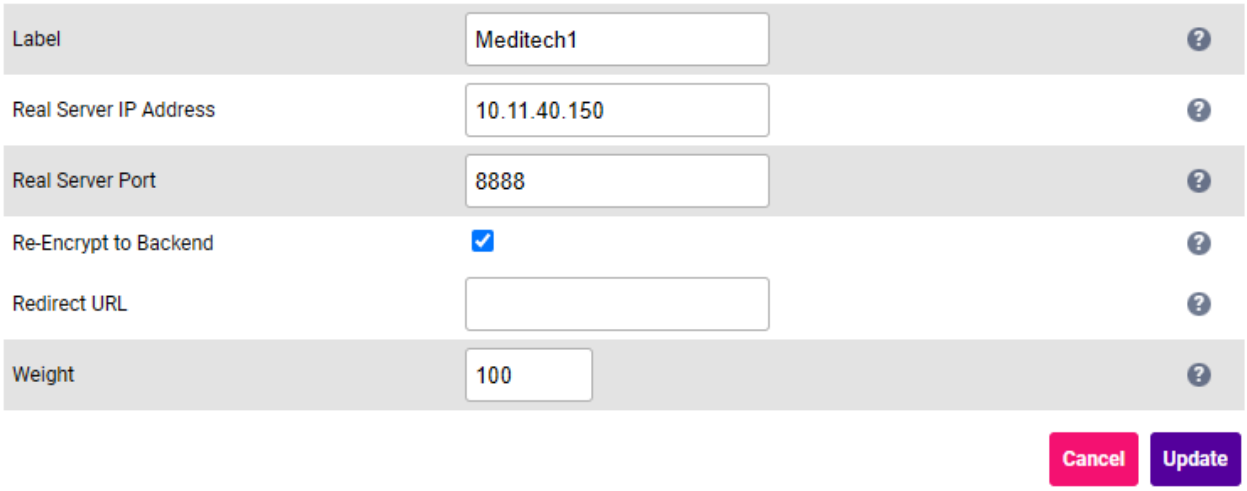
1. Using the WebUI, navigate to *Cluster Configuration > Layer 7 – Virtual Services* and click on **Add a new Virtual Service**.
2. Enter the following details:



3. Define the *Label* for the Virtual Service as required, e.g. **Meditech-APP**.
4. Set the *Virtual Service IP Address* field to the required IP address, e.g. **10.11.40.141**.
5. Set the *Ports* field to **80**.
6. Set the *Layer 7 Protocol* to **HTTP Mode**.
7. Click **Update** to create the Virtual Service.
8. Now click **Modify** next to the newly created VIP.
9. Scroll to the *Persistence* section.
    - Set the *Persistence Mode* to **None**.
10. Scroll to the *Health Checks* section.
    - Set the *Health Checks* to **Negotiate HTTPS (HEAD)**.
11. Scroll to the *SSL* section.
    - Enable (check) *Enable Backend Encryption*.
12. Scroll to the *Other* section and click **[Advanced]**.
    - Set *Force to HTTPS* to **Yes**.
13. Leave all other settings at their default value.
14. Click **Update**.

11.2.2. Define the Associated Real Servers (RIPs)

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



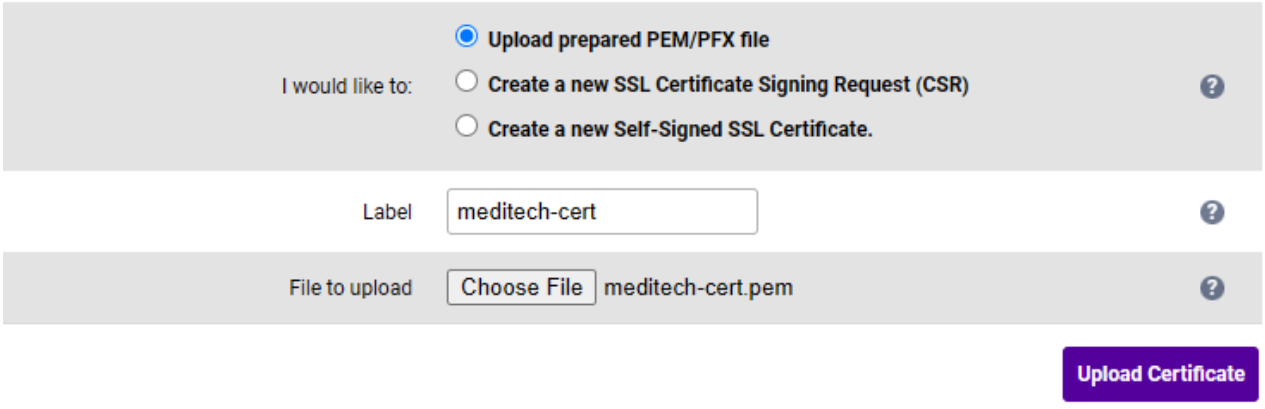
3. Define the *Label* for the Real Server as required, e.g. **Meditech1**.
4. Set the *Real Server IP Address* field to the required IP address, e.g. **10.11.40.150**.
5. Set the *Real Server Port* field to **8888**.
6. Leave all other settings at their default value.
7. Click **Update**.
8. Repeat these steps to add the remaining Meditech server(s).

11.3. Upload the SSL Certificate

Certificates in either PEM or PFX format can be uploaded.

> **Note** If the API and APP services use a different certificate, run through the steps below twice to upload both certs. Use a relevant label (name) for each certificate.

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:

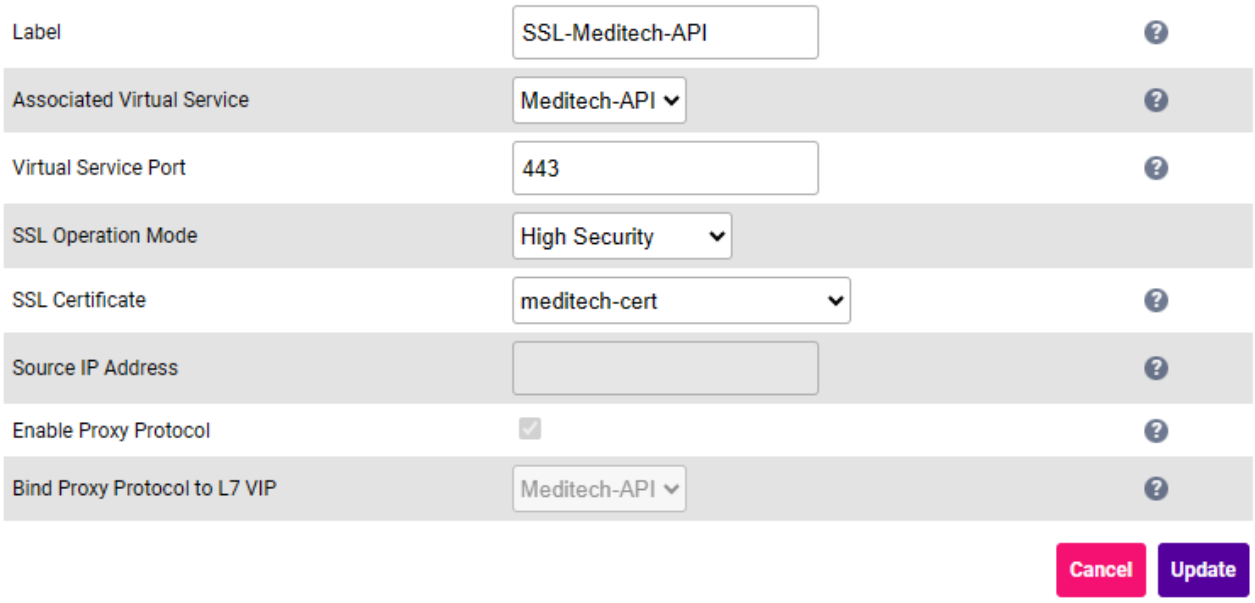


4. Specify an appropriate *Label*, e.g. **meditech-cert**.

5. Click **Choose File**.
6. Browse to and select the relevant PEM or PFX file.
7. For PFX files specify the password if required.
8. Click **Upload Certificate**.

11.4. Configure SSL Termination

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



3. Using the *Associated Virtual Service* drop-down, select the Virtual Service created above, e.g. **Medtech-API**.

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

4. Ensure that the *Virtual Service Port* is set to **443**.
5. Leave *SSL Operation Mode* set to **High Security**.
6. Select the relevant *SSL Certificate* uploaded previously.
7. Leave all other settings at their default value.
8. Click **Update**.
9. Now repeat these steps to configure the SSL termination for the **Meditech-APP** VIP.

12. Finalizing the Configuration

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

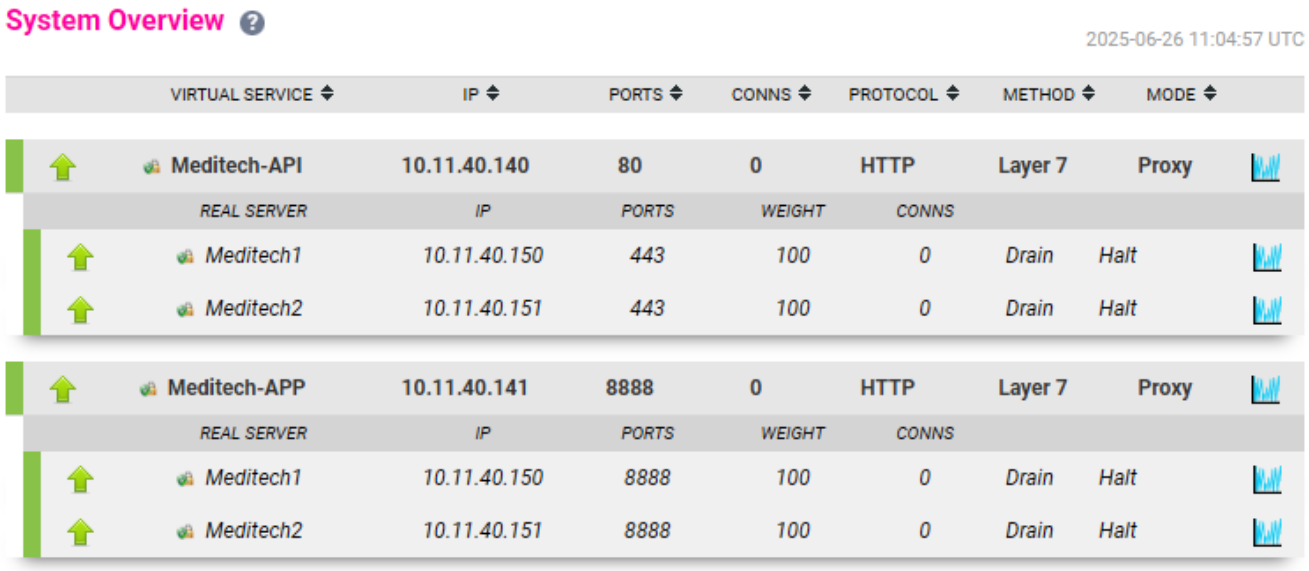
1. Using the WebUI, navigate to: *Maintenance > Restart Services*.
2. Click **Reload HAProxy**.
3. Click **Reload STunnel**.

13. Testing & Verification

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

13.1. Using System Overview

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



> **Note** The image above shows Option 2 - SSL Bridging. Padlock icons are displayed on both Virtual Services and all Real Servers to indicate that frontend SSL termination and backend re-encryption is enabled.

14. Technical Support

For more details about configuring the appliance and assistance with designing your deployment please don't hesitate to contact the support team using the following email address: support@loadbalancer.org.

15. Further Documentation

For additional information, please refer to the Administration Manual.

16. Appendix

16.1. 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.

> **Note** For Enterprise Azure, the HA pair should be configured first. For more information, please refer to the Azure Quick Start/Configuration Guide available in the documentation library

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.

16.1.1. 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:

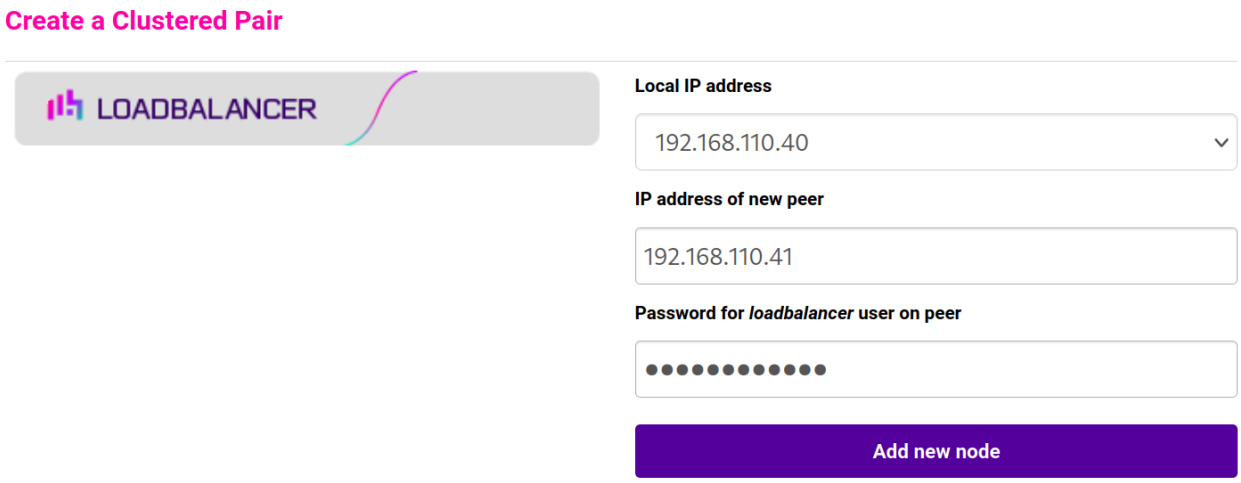
WebUI Main Menu Option	Sub Menu Option	Description
Local Configuration	Hostname & DNS	Hostname and DNS settings
Local Configuration	Network Interface Configuration	Interface IP addresses, bonding configuration and VLANs
Local Configuration	Routing	Default gateways and static routes
Local Configuration	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	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.

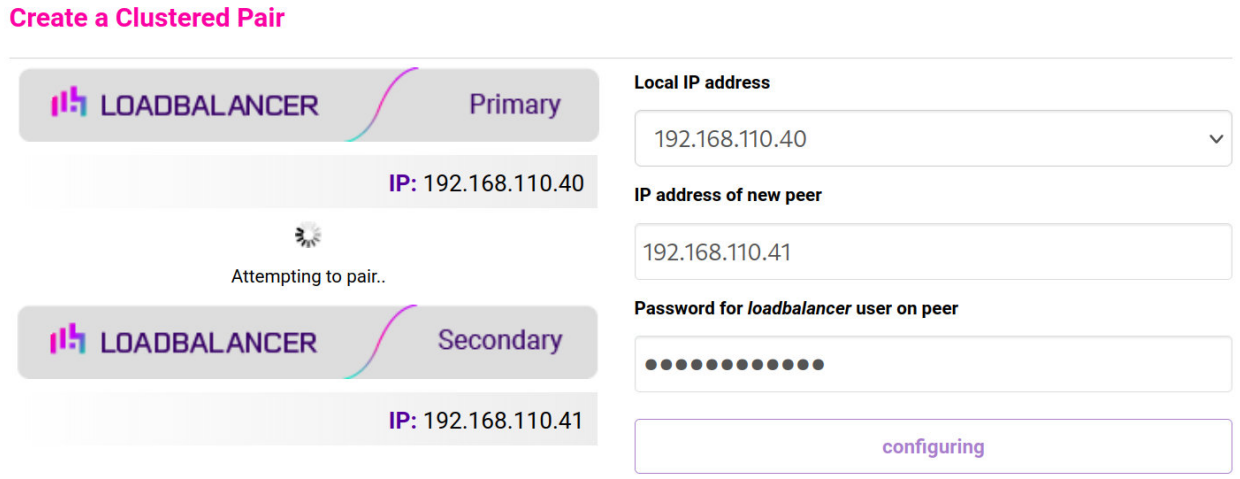
16.1.2. Configuring the HA Clustered Pair

> **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.

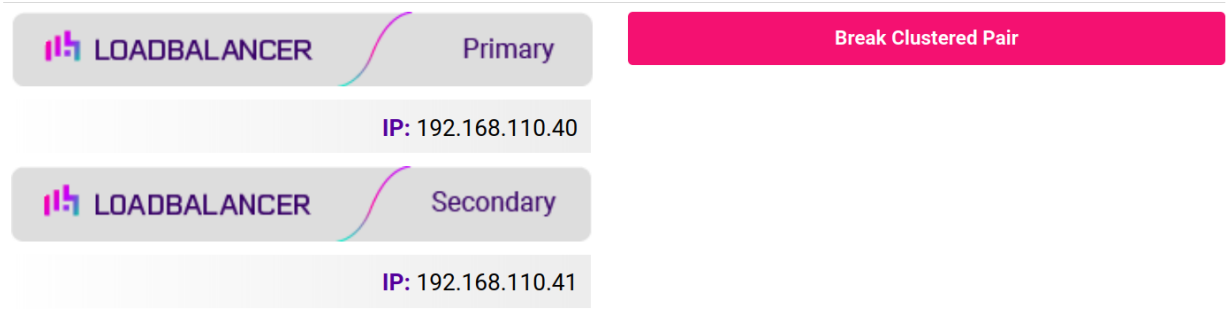
1. Deploy a second appliance that will be the Secondary and configure initial network settings.
2. Using the WebUI on the Primary appliance, navigate to: *Cluster Configuration > High-Availability Configuration*.



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:



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



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.

17. Document Revision History

Version	Date	Change	Reason for Change	Changed By
1.0.0	1 October 2019	Initial version		IG
1.0.1	11 February 2021	New title page Updated Canadian contact details	Branding update Change to Canadian contact details	AH
1.1.0	1 December 2021	Converted the document to AsciiDoc	Move to new documentation system	AH, RJC, ZAC
1.1.1	22 April 2022	Updated SSL related content to reflect latest software version	New software release	RJC
1.1.2	28 September 2022	Updated layer 7 VIP and RIP creation screenshots	Reflect changes in the web user interface	AH
1.1.3	5 January 2023	Combined software version information into one section Added one level of section numbering Added software update instructions Added table of ports used by the appliance Reworded 'Further Documentation' section Removed references to the colour of certain UI elements	Housekeeping across all documentation	AH
1.1.4	2 February 2023	Updated screenshots	Branding update	AH
1.1.5	7 March 2023	Removed conclusion section	Updates across all documentation	AH
1.2.0	24 March 2023	New document theme Modified diagram colours	Branding update	AH

Version	Date	Change	Reason for Change	Changed By
1.3.0	1 July 2025	Various technical changes to align wth Meditech documentation Improved document layout & structure Removed superfluous content Removed erroneous formatting characters	Technical accuracy & readability	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.