

Load Balancing Fujifilm SYNAPSE

Version 1.4.0



Table of Contents

1. About this Guide	4
2. Loadbalancer.org Appliances Supported	4
3. Software Versions Supported	4
3.1. Loadbalancer.org Appliance	4
3.2. Fujifilm Synapse	4
4. Load Balancing Fujifilm Synapse	4
4.1. Port Requirements	
4.2. Deployment Concept	5
4.3. Virtual Service (VIP) Requirements	
Synapse PACS	
Synapse VNA	
Synapse Mobility	
Synapse CWM.	
4.4. Synapse Server Configuration Requirements	
SNAT Mode	
DR Mode.	
5. Loadbalancer.org Appliance – the Basics	
5.1. Virtual Appliance	
5.2. Initial Network Configuration	
5.3. Accessing the Appliance WebUI	
Main Menu Options	
5.4. Appliance Software Update.	
Determining the Current Software Version	
Checking for Updates using Online Update.	
5.5. Ports Used by the Appliance.	
5.6. HA Clustered Pair Configuration	
6. Load Balancing Fujifilm Synapse PACS.	
6.1. Appliance Configuration	
Configuring VIP1 - synapsePacsHTTP.	
Configuring VIP2 - synapsePacsDICOM	
6.2. Synapse PACS Configuration	
7. Load Balancing Fujifilm Synapse VNA	
7.1. Appliance Configuration	
Configuring VIP1 - synapseVnaHTTP	
Configuring VIP2 - synapseVnaDICOM	
7.2. Synapse VNA Configuration	
8. Load Balancing Fujifilm Synapse Mobility	
8.1. Appliance Configuration	
Configuring VIP1 - synapseMobility	
8.2. Synapse Mobility Configuration	19
9. Load Balancing Fujifilm Synapse CWM	19
9.1. Appliance Configuration	
Configuring VIP1 - SynapseCwm	19
9.2. Synapse CWM Configuration	21
10. Finalizing the Configuration	21
11. Additional Configuration Options & Settings	21
11.1. SSL Termination	21

11.2. SSL Termination on the load balancer - SSL Offloading	21
Certificates	22
Uploading Certificates	22
11.3. Configuring SSL Termination on the Load Balancer	23
1) Configuring SSL Offloading for Synapse Mobility using a Layer 7 HTTP mode VIP	23
2) Configure SSL termination	24
Finalizing the Configuration	25
12. Testing & Verification	26
12.1. Using the System Overview	26
12.2. Client Connection Tests	26
13. Technical Support	26
14. Additional Documentation	26
15. Appendix	27
15.1. Configuring HA - Adding a Secondary Appliance	27
Non-Replicated Settings	27
Adding a Secondary Appliance - Create an HA Clustered Pair	28
15.2. DR Mode Server Configuration	29
Windows Server 2012 & Later	29
16. Document Revision History	35

1. About this Guide

This guide details the steps required to configure a load balanced Fujifilm Synapse environment utilizing Loadbalancer.org appliances. It covers Synapse PACS, Synapse VNA, Synapse Mobility and Synapse CWM and details the configuration of the load balancers and also any Synapse server 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 Fujifilm Synapse. For full specifications of available models please refer to https://www.loadbalancer.org/products.

Some features may not be supported in all cloud platforms due to platform specific limitations, please check with Loadbalancer.org support for further details.

3. Software Versions Supported

3.1. Loadbalancer.org Appliance

V8.3.8 and later

8 Note

The screenshots used throughout this document aim to track the latest Loadbalancer.org software version. If using an older software version, note that the screenshots presented here may not match the WebUI exactly.

3.2. Fujifilm Synapse

- Fujifilm Synapse PACS All versions
- Fujifilm Synapse VNA All versions
- Fujifilm Synapse Mobility All versions
- Fujifilm Synapse CWM All versions

4. Load Balancing Fujifilm Synapse

For high availability and scalability, Fujifilm recommend that multiple Synapse Servers are deployed in a load balanced cluster.

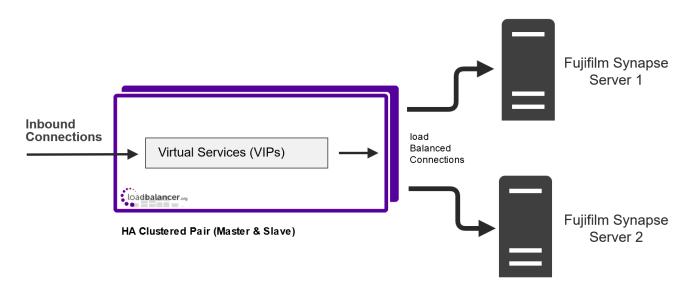
4.1. Port Requirements

The following table shows the ports used by the various Synapse systems. The load balancer must be configured to listen on the same ports.

Port	Protocols	System	Use
80	TCP	PACS	НТТР
104	TCP	PACS	DICOM
80	TCP	VNA	HTTP
104	TCP	VNA	DICOM
8080	TCP	Mobility	НТТР
8443	TCP	Mobility	HTTPS
80	TCP	CWM	НТТР

4.2. Deployment Concept

When Fujifilm systems are deployed with the load balancer, clients connect to the Virtual Service (VIP) on the load balancer rather than connecting directly to one of the Fujifilm servers. The load balancer then distributes these connection to the load balanced servers according to the algorithm selected.



8 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 Configuring HA - Adding a Secondary Appliance for more details on configuring a clustered pair.

4.3. Virtual Service (VIP) Requirements

The following tables summarize the VIPs required for each Synapse system and how they are configured.

Synapse PACS

2 VIPs are required:

Ref.	VIP Name	Operating Mode	Protocol	Port(s)	Persistence	Health check Type
VIP1	SynapsePacsHTTP	Layer 7 SNAT mode	TCP	80	Source IP	Connect to Port

Ref.	VIP Name	Operating Mode	Protocol	Port(s)	Persistence	Health check Type
VIP2	SynapsePacsDICO M	Layer 4 DR mode	TCP	104		External Script – DICOM-C-ECHO

Synapse VNA

2 VIPs are required:

Ref.	VIP Name	Operating Mode	Protocol	Port(s)	Persistence	Health check Type
VIP1	SynapseVnaHTTP	Layer 7 SNAT mode	TCP	80	Source IP	Connect to Port
VIP2	SynapseVnaDICOM	Layer 4 DR mode	TCP	104	Source IP	External Script – DICOM-C-ECHO

Synapse Mobility

1 VIP is required:

R	Ref.	VIP Name	Operating Mode	Protocol	Port(s)	Persistence	Health check Type
V	/IP1	SynapseMobility	Layer 7 SNAT mode	TCP	8080 8443	Source IP	Negotiate HTTP (GET)

Synapse CWM

1 VIP is required:

Ref.	VIP Name	Operating Mode	Protocol	Port(s)	Persistence	Health check Type
VIP1	SynapseCwm	Layer 7 SNAT mode	HTTP	80	HTTP Cookie	Connect to Port

4.4. Synapse Server Configuration Requirements

As mentioned in the tables above, Layer 7 SNAT mode and Layer 4 DR mode are used when load balancing Fujifilm Synapse.

SNAT Mode

When using Layer 7 SNAT mode, no mode-specific Synapse server configuration changes are required.

DR Mode

When using DR mode, the 'ARP problem' must be solved on each Synapse server for DR mode to work. For detailed steps on solving the ARP problem, please refer to DR Mode Server Configuration for more information.

5. Loadbalancer.org Appliance – the Basics

5.1. 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.

8 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.
8 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.
8 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.

5.2. Initial Network Configuration

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

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

5.3. 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.

8 Note	There are certain differences when accessing the WebUI for the cloud appliances. For details, please refer to the relevant Quick Start / Configuration Guide.
8 Note	A number of compatibility issues have been found with various versions of Microsoft Internet Explorer and Edge. The WebUI has been tested and verified using both Chrome & Firefox.

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

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

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

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



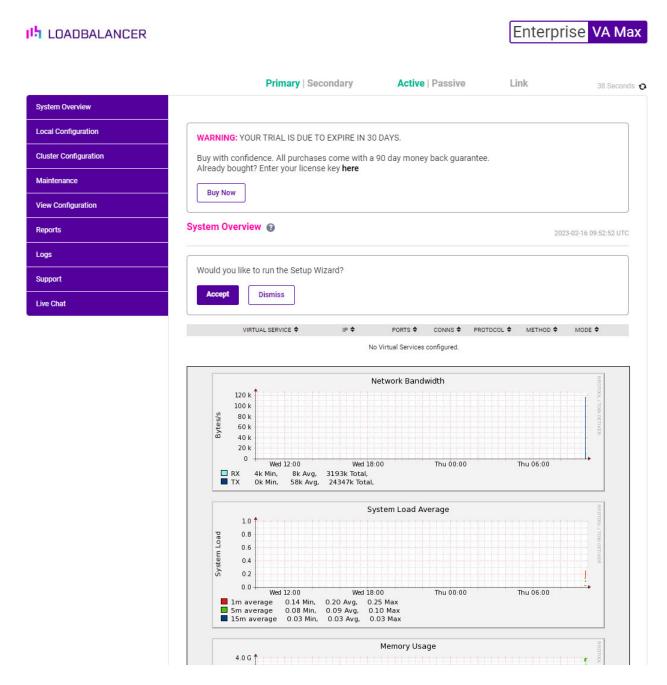
Username: loadbalancer

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

8 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.

8 Note

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

Main Menu Options



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

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

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

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

View Configuration - Display the saved appliance configuration settings

Reports - View various appliance reports & graphs

Logs - View various appliance logs

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

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

5.4. Appliance Software Update

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

Determining the Current Software Version

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

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



Checking for Updates using Online Update

8 Note

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

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

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

- 4. If an update is available, you'll be presented with a list of new features, improvements, bug fixes and security related updates.
- 5. Click **Online Update** to start the update process.
 - Note Do not navigate away whilst the update is ongoing, this may cause the update to fail.
- 6. Once complete (the update can take several minutes depending on download speed and upgrade version) the following message will be displayed:

Information: Update completed successfully.

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

Using Offline Update

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

8 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
Upload and Install

- 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.

5.5. 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
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	9080	WebUI - HTTP (disabled by default)
TCP	9081	Nginx fallback page
TCP	9443	WebUI - HTTPS

5.6. 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.

6. Load Balancing Fujifilm Synapse PACS

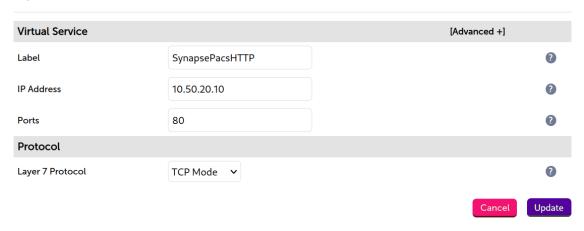
6.1. Appliance Configuration

Configuring VIP1 - synapsePacsHTTP

a) Setting up the Virtual Service

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

Layer 7 - Add a new Virtual Service



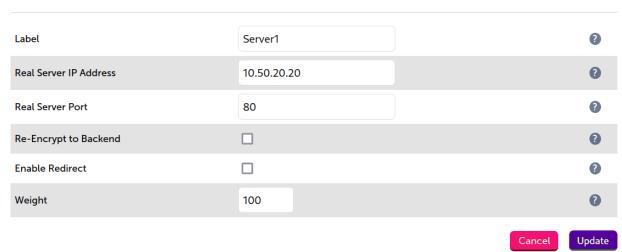
- 3. Enter an appropriate label for the VIP, e.g. **SynapsPacsHTTP**.
- 4. Set the Virtual Service IP address field to the required IP address, e.g. 10.50.20.10.
- 5. Set the Virtual Service Ports field to 80.
- 6. Set Layer 7 Protocol to TCP Mode.

7. Click Update.

b) Setting up the Real Servers

- 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:

Layer 7 Add a new Real Server

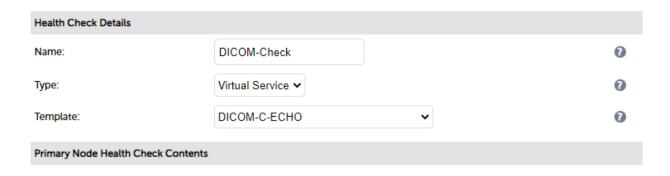


- 3. Enter an appropriate label for the RIP, e.g. **Server1**.
- 4. Set the Real Server IP Address field to the required IP address, e.g. 10.50.20.20.
- 5. Set the Real Server Port field to 80.
- 6. Click Update.
- 7. Repeat the above steps to add your other server(s).

Configuring VIP2 - synapsePacsDICOM

a) Configure the DICOM health check

1. Using the WebUI, navigate to *Cluster Configuration > Health Check Scripts* and click **Add New Health Check**.

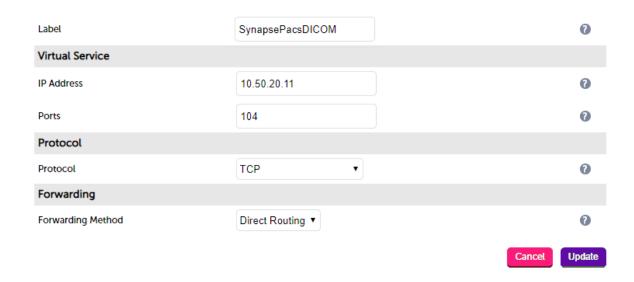


- 2. Specify an appropriate *Name* for the health check, e.g. **DICOM-Check**.
- 3. Set *Type* to **Virtual Service**.

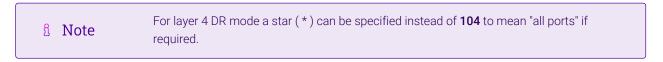
- 4. Set Template to DICOM-C-ECHO.
- 5. Click Update.

b) Setting up the Virtual Service (VIP)

- 1. Using the WebUI, navigate to: *Cluster Configuration > Layer 4 Virtual Services* and click **Add a new Virtual Service**.
- 2. Enter the following details:



- 3. Enter an appropriate label (name) for the VIP, e.g. SynapsePacsDICOM.
- 4. Set the Virtual Service IP address field to the required IP address, e.g. 10.50.20.11.
- 5. Set the Virtual Service Ports field to 104.



- 6. Leave Protocol set to TCP.
- 7. Leave the *Forwarding Method* to **Direct Return**.
- 8. Click Update.
- 9. Now click **Modify** next to the newly created Virtual Service.
- 10. Scroll down to the *Health Checks* section.
 - a. Set Check Type to External script.
 - b. Set External Script to DICOM-Check.
- 11. Click Update.

c) Setting up the Real Server (RIP)

1. Using the WebUI, navigate to: *Cluster Configuration > Layer 4 – Real Servers* and click **Add a new Real**Server next to the newly created VIP.

2. Enter the following details:



- 3. Enter an appropriate label (name) for the RIP, e.g. Server1.
- 4. Change the Real Server IP Address field to the required IP address, e.g. 10.50.20.21.
- 5. Click **Update**.
- 6. Repeat the above steps to add your other server(s).

6.2. Synapse PACS Configuration

Since VIP2 is configured using layer 4 DR (Direct Return) mode, the "ARP Problem" must be solved on each Synapse server as mentioned in DR Mode. For full details on how this is done, please refer to DR Mode Server Configuration.

7. Load Balancing Fujifilm Synapse VNA

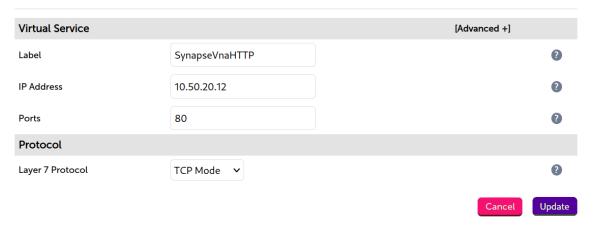
7.1. Appliance Configuration

Configuring VIP1 - synapseVnaHTTP

a) Setting up the Virtual Service

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

Layer 7 - Add a new Virtual Service

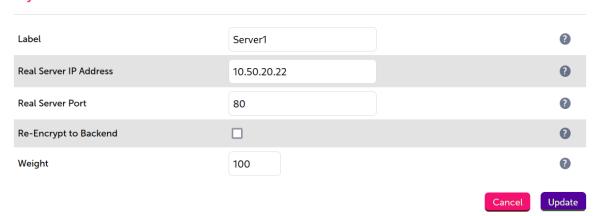


- 3. Enter an appropriate label for the VIP, e.g. **SynapseVnaHTTP**.
- 4. Set the *Virtual Service IP address* field to the required IP address, e.g. **10.50.20.12**.
- 5. Set the Virtual Service Ports field to 80.
- 6. Set Layer 7 Protocol set to TCP Mode.
- 7. Click **Update**.

b) Setting up the Real Servers

- 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:

Layer 7 Add a new Real Server



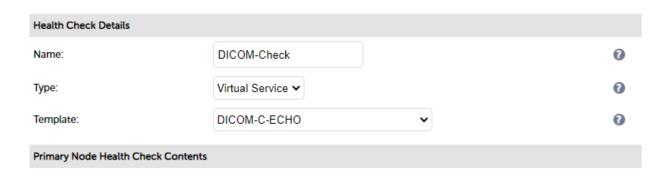
- 3. Enter an appropriate label for the RIP, e.g. **Server1**.
- 4. Set the Real Server IP Address field to the required IP address, e.g. 10.50.20.22.
- 5. Set the Real Server Port field to 80.
- 6. Click **Update**.
- 7. Repeat the above steps to add your other server(s).

Configuring VIP2 - synapseVnaDICOM

a) Configure the DICOM health check



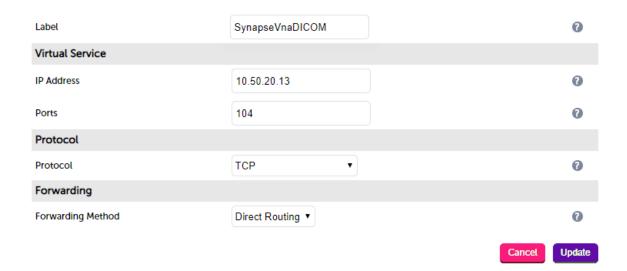
1. Using the WebUI, navigate to *Cluster Configuration > Health Check Scripts* and click **Add New Health Check**.



- 2. Specify an appropriate *Name* for the health check, e.g. **DICOM-Check**.
- 3. Set *Type* to **Virtual Service**.
- 4. Set Template to DICOM-C-ECHO.
- 5. Click **Update**.

b) Setting up the Virtual Service (VIP)

- 1. Using the WebUI, navigate to: *Cluster Configuration > Layer 4 Virtual Services* and click **Add a new Virtual Service**.
- 2. Enter the following details:



- 3. Enter an appropriate label (name) for the VIP, e.g. SynapseVnaDICOM.
- 4. Set the Virtual Service IP address field to the required IP address, e.g. 10.50.20.13.
- 5. Set the Virtual Service Ports field to 104.

Note

For layer 4 DR mode a star (*) can be specified instead of **104** to mean "all ports" if required.

- 6. Leave Protocol set to TCP.
- 7. Leave the *Forwarding Method* to **Direct Return**.
- 8. Click Update.
- 9. Now click **Modify** next to the newly created Virtual Service.
- 10. Scroll down to the Health Checks section.
 - a. Set Check Type to External script.
 - b. Set *External Script* to **DICOM-Check**.
- 11. Click Update.

c) Setting up the Real Server (RIP)

- 1. Using the WebUI, navigate to: *Cluster Configuration > Layer 4 Real Servers* and click **Add a new Real**Server next to the newly created VIP.
- 2. Enter the following details:



- 3. Enter an appropriate label (name) for the RIP, e.g. Server1.
- 4. Change the Real Server IP Address field to the required IP address, e.g. 10.50.20.23.
- 5. Click Update.
- 6. Repeat the above steps to add your other server(s).

7.2. Synapse VNA Configuration

Since VIP2 is configured using layer 4 DR (Direct Return) mode, the "ARP Problem" must be solved on each Synapse server as mentioned in DR Mode. For full details on how this is done, please refer to DR Mode Server Configuration.

8. Load Balancing Fujifilm Synapse Mobility



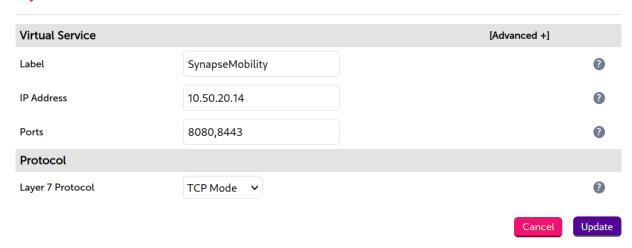
8.1. Appliance Configuration

Configuring VIP1 - synapseMobility

a) Setting up the Virtual Service

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

Layer 7 - Add a new Virtual Service

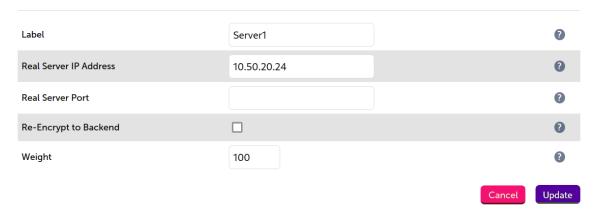


- 3. Enter an appropriate label for the VIP, e.g. SynapseMobility.
- 4. Set the Virtual Service IP address field to the required IP address, e.g. 10.50.20.14.
- 5. Set the Virtual Service Ports field to 8080,8443.
- 6. Set Layer 7 Protocol set to TCP Mode.
- 7. Click **Update**.
- 8. Scroll down to the *Health Checks* section and set the *Health Check* to **Negotiate HTTP (GET)**.
- 9. Set Request to Send to https://syncavmob:8080/pureweb/server/login.jsp.
- 10. Leave Response Expected blank (this will configure the load balancer to look for a 200 OK response).

b) Setting up the Real Servers

- 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:

Layer 7 Add a new Real Server



- 3. Enter an appropriate label for the RIP, e.g. **Server1**.
- 4. Set the Real Server IP Address field to the required IP address, e.g. 10.50.20.24.
- 5. Leave the *Real Server Port* field blank.
- 6. Click **Update**.
- 7. Repeat the above steps to add your other server(s).

8.2. Synapse Mobility Configuration

As mentioned in SNAT Mode, when using Layer 7 SNAT mode no mode-specific Synapse server configuration changes are required.

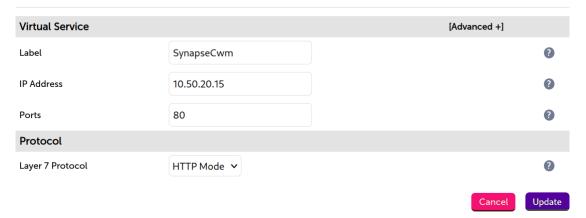
9. Load Balancing Fujifilm Synapse CWM

9.1. Appliance Configuration

Configuring VIP1 - SynapseCwm

- a) Setting up the Virtual Service
 - 1. Using the WebUI, navigate to: *Cluster Configuration > Layer 7 Virtual Service* and click **Add a New Virtual Service**.
 - 2. Enter the following details:

Layer 7 - Add a new Virtual Service

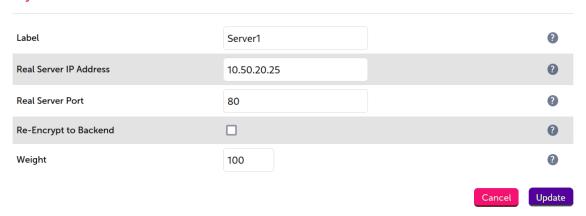


- 3. Enter an appropriate label for the VIP, e.g. SynapseCwm.
- 4. Set the Virtual Service IP address field to the required IP address, e.g. 10.50.20.15.
- 5. Set the Virtual Service Ports field to 80.
- 6. Set Layer 7 Protocol set to HTTP Mode.
- 7. Click Update.

b) Setting up the Real Servers

- 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:

Layer 7 Add a new Real Server



- 3. Enter an appropriate label for the RIP, e.g. Server1.
- 4. Set the Real Server IP Address field to the required IP address, e.g. 10.50.20.25.
- 5. Set the *Real Server Port* field to **80**.
- 6. Click **Update**.
- 7. Repeat the above steps to add your other server(s).

9.2. Synapse CWM Configuration

As mentioned in SNAT Mode, when using Layer 7 SNAT mode no mode-specific Synapse server configuration changes are required.

10. Finalizing the Configuration

Once all the VIPs have been configured, HAProxy must be reloaded to apply the new settings (for Layer 7 VIPs). 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.

11. Additional Configuration Options & Settings

11.1. SSL Termination

SSL termination can be handled in the following ways:

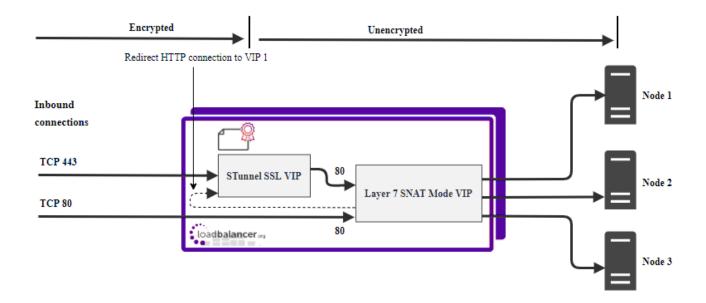
- 1. On the Real Servers aka SSL Pass-through
- 2. On the load balancer aka SSL Offloading
- 3. On the load balancer with re-encryption to the backend servers aka SSL Bridging

By default, a self-signed certificate is used for the new SSL VIP. Certificates can be requested on the load balancer or uploaded as described in the section below. The default self-signed certificate can be regenerated if needed using the WebUI menu option: SSL Certificate and clicking the Regenerate Default Self Signed Certificate button.

The backend for the SSL VIP can be either a Layer 7 SNAT mode VIP or a Layer 4 NAT or SNAT

The backend for the SSL VIP can be either a Layer 7 SNAT mode VIP or a Layer 4 NAT or SNAT mode VIP. Layer 4 DR mode cannot be used since stunnel acts as a proxy, and the VPSA node servers see requests with a source IP address of the VIP. However, since the VPSA node servers believe that they own the VIP (due to the loopback adapter configured to handle to ARP problem) they are unable to reply to stunnel.

11.2. SSL Termination on the load balancer - SSL Offloading



In this case, an SSL VIP utilizing stunnel is configured on the appliance and an SSL certificate is uploaded and associated to the Virtual Service. Data is encrypted from the client to the load balancer, but is un-encrypted from the load balancer to the backend servers as shown above.

Certificates

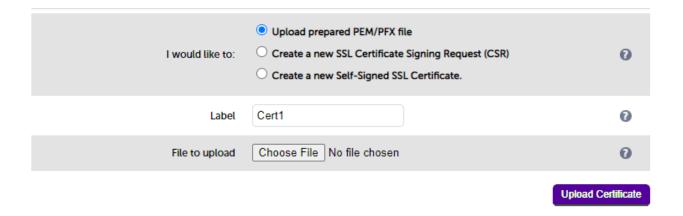
If you already have an SSL certificate in either PFX or PEM file format, this can be uploaded to the Load balancer using the certificate upload option as explained below in Uploading Certificates. Alternatively, you can create a Certificate Signing Request (CSR) on the load balancer and send this to your CA to create a new certificate. For more information please refer to Generating a CSR on the Load Balancer.

Uploading Certificates

If you already have a certificate in either PEM or PFX format, this can be uploaded to the load balancer.

To upload a Certificate:

- 1. Using the WebUI, navigate to: Cluster Configuration > SSL Certificates.
- 2. Click Add a new SSL Certificate & select Upload prepared PEM/PFX file.



- 3. Enter a suitable Label (name) for the certificate, e.g. Cert1.
- 4. Browse to and select the certificate file to upload (PEM or PFX format).
- 5. Enter the password if applicable.
- 6. Click **Upload Certificate**, if successful, a message similar to the following will be displayed:

Information: cert1 SSL Certificate uploaded successfully.

8 Note

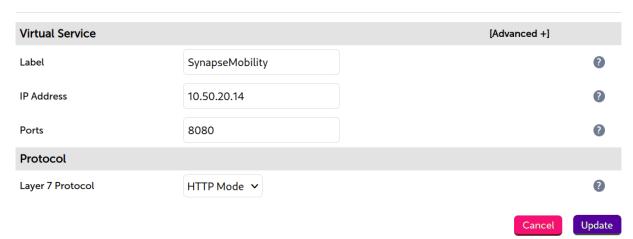
To backup your certificates use the WebUI menu option: *Maintenance > Backup & Restore > Download SSL Certificates*.

11.3. Configuring SSL Termination on the Load Balancer

To configure SSL termination for Synapse Mobility:

- 1. Configure a layer 7 HTTP mode VIP to handle HTTP traffic
- 2. Configure SSL termination to handle HTTPS traffic
- 1) Configuring SSL Offloading for Synapse Mobility using a Layer 7 HTTP mode VIP
- a) Setting up the Virtual Service (VIP)
 - 1. Using the WebUI, navigate to *Cluster Configuration > Layer 7 Virtual Services* and click **Add a new Virtual Service**.
 - 2. Enter the following details:

Layer 7 - Add a new Virtual Service

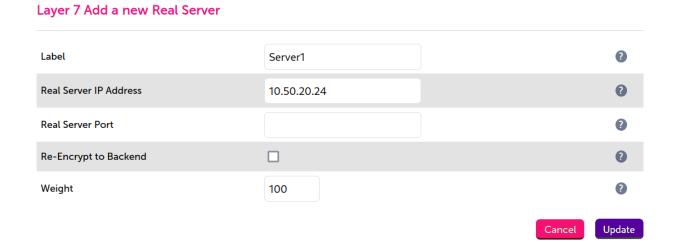


- 3. Enter an appropriate label for the VIP, e.g. **SynapseMobility**.
- 4. Set the Virtual Service IP address field to the required IP address, e.g. 10.50.20.14.
- 5. Set the Virtual Service Ports field to 8080.

- 6. Set Layer 7 Protocol to HTTP Mode.
- 7. Click Update.
- 8. Click Modify.
- 9. Scroll down to the *Health Checks* section and set the *Health Check* to **Negotiate HTTP (GET)**.
- 10. Set Request to Send to https://syncavmob:8080/pureweb/server/login.jsp.
- 11. Leave Response Expected blank (this will configure the load balancer to look for a 200 OK response).

b) Setting up the Real Servers

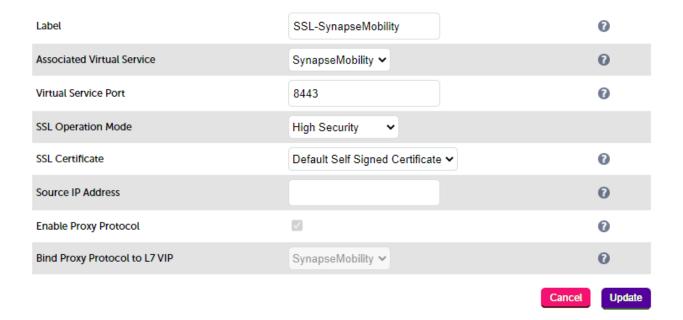
- 1. Using the WebUI, navigate to: *Cluster Configuration > Layer 7 Real Servers* and click **Add a new Real**Server next to the newly created VIP.
- 2. Enter the following details:



- 3. Enter an appropriate label for the RIP, e.g. Server1.
- 4. Set the Real Server IP Address field to the required IP address, e.g. 10.50.20.24.
- 5. Leave the *Real Server Port* field blank.
- 6. Click Update.
- 7. Repeat the above steps to add your other server(s).

2) Configure SSL termination

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



2. Set *Associated Virtual Service* to the appropriate VIP, e.g. **SynapseMobility**. This will automatically fill in the label as the VIP name with SSL inserted in front of the VIP name e.g. **SSL-SynapseMobility**.

8 Note

The Associated Virtual Service drop-down is populated with all single port, standard (i.e. non-manual) Layer 7 VIPs available on the load balancer. Using a Layer 7 VIP for the backend is the recommended method although as mentioned earlier, Layer 4 NAT mode and layer 4 SNAT mode VIPs can also be used if required. To forward traffic from the SSL VIP to these type of VIPs, you'll need to set Associated Virtual Service to **Custom**, then configure the IP address & port of the required VIP.

- 3. Set Virtual Service Port to 8443.
- 4. Leave SSL operation Mode set to High Security.
- 5. Select the required certificate from the SSL Certificate drop-down.
- 6. Click Update.

Once configured, HTTP traffic will be load balanced by the Layer 7 SNAT mode VIP and HTTPS traffic will be terminated by the SSL VIP, then passed on to the Layer 7 SNAT mode VIP as unencrypted HTTP for load balancing.

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.

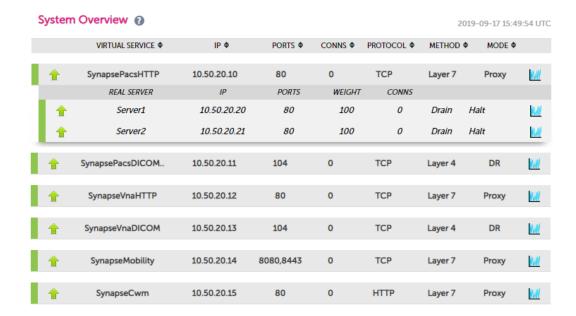
12. Testing & Verification

8 Note

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

12.1. Using the System Overview

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



12.2. Client Connection Tests

Ensure that clients can connect via the load balancer to the Synapse servers. You'll probably need to create new DNS records or modify your existing DNS records, replacing the IP addresses of individual servers or the cluster with the IP address of the Virtual Service on the load balancer.

13. 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.

14. Additional Documentation

For additional information, please refer to the Administration Manual.

15. Appendix

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

8 Note

For Enterprise Azure, the HA pair should be configured first. In Azure, when creating a VIP using an HA pair, 2 private IPs must be specified – one for the VIP when it's active on the Primary and one for the VIP when it's active on the Secondary. Configuring the HA pair first, enables both IPs to be specified when the VIP is created.

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

Non-Replicated Settings

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

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

(!) Important

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

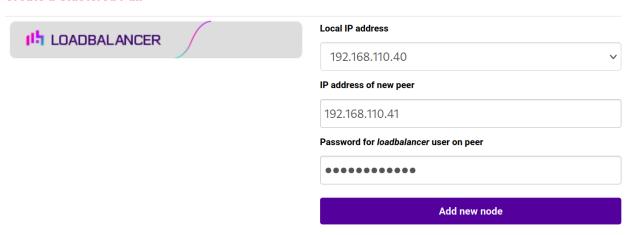
Adding a Secondary Appliance - Create an HA Clustered Pair

8 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.

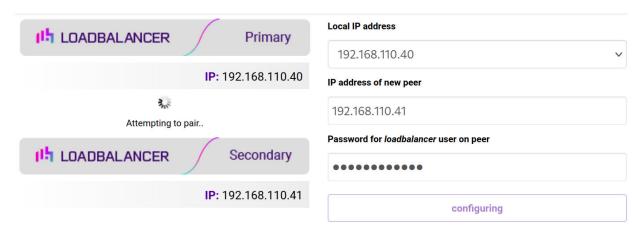
- 1. Deploy a second appliance that will be the Secondary and configure initial network settings.
- 2. Using the WebUI on the Primary appliance, navigate to: *Cluster Configuration > High-Availability Configuration*.

Create a Clustered Pair



- 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



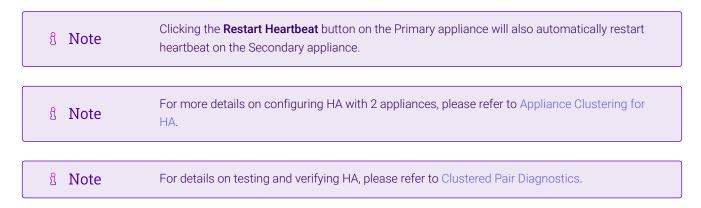
6. Once complete, the following will be displayed on the Primary appliance:



High Availability Configuration - primary



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.



15.2. DR Mode Server Configuration

When using Layer 4 DR mode the ARP problem must be solved. This involves configuring each Synapse Server to accept traffic destined for the VIP in addition to it's own IP address, and ensuring that each server does not respond to ARP requests for the VIP address – only the load balancer should do this. The following section covers Windows 2012 and later, for earlier versions of Windows please refer to the Administration Manual.

Windows Server 2012 & Later

Windows Server 2012 and later support Direct Routing (DR) mode through the use of the Microsoft Loopback Adapter that must be installed and configured on each load balanced (Real) Server. The IP address configured on the Loopback Adapter must be the same as the Virtual Service (VIP) address. This enables the server to receive packets that have their destination set as the VIP address. If a Real Server is included in multiple DR mode VIPs, an IP address for each VIP must be added to the Loopback Adapter.

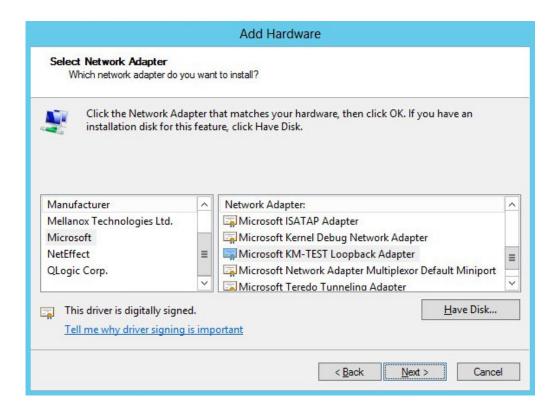
In addition, steps must be taken to set the strong/weak host behavior on each Real Server. This is used to either prevent or allow interfaces to receive packets destined for a different interface on the same server.

(1) Important The following 3 steps must be completed on **all** Real Servers associated with the VIP.

Step 1 of 3: Install the Microsoft Loopback Adapter

- 1. Click **Start**, then run **hdwwiz** to start the Hardware Installation Wizard.
- 2. Once the Wizard has started, click Next.

- 3. Select Install the hardware that I manually select from a list (Advanced), click Next.
- 4. Select Network adapters, click Next.



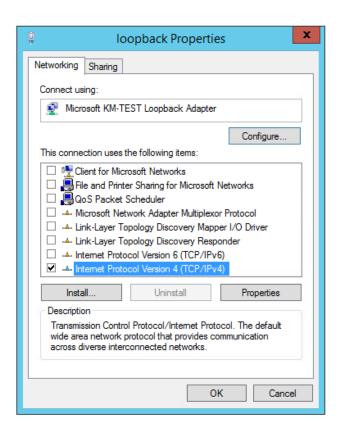
- 5. Select Microsoft & Microsoft KM-Test Loopback Adapter, click Next.
- 6. Click **Next** to start the installation, when complete click **Finish**.

Step 2 of 3: Configure the Loopback Adapter

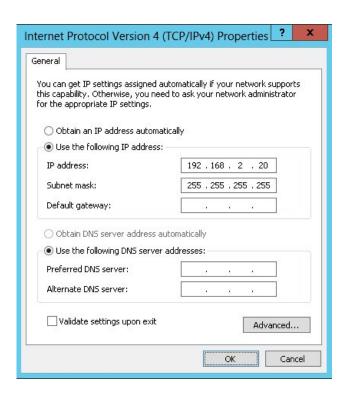
- 1. Open Control Panel and click **Network and Sharing Center**.
- 2. Click Change adapter settings.
- 3. Right-click the new Loopback Adapter and select Properties.
- Note You can configure IPv4 or IPv6 addresses or both depending on your requirements.

IPv4 Addresses

1. Uncheck all items except Internet Protocol Version 4 (TCP/IPv4) as shown below:



2. Ensure that Internet Protocol Version (TCP/IPv4) is selected, click Properties and configure the IP address to be the same as the Virtual Service address (VIP) with a subnet mask of 255.255.255.255, e.g. 192.168.2.20/255.255.255.255 as shown below:

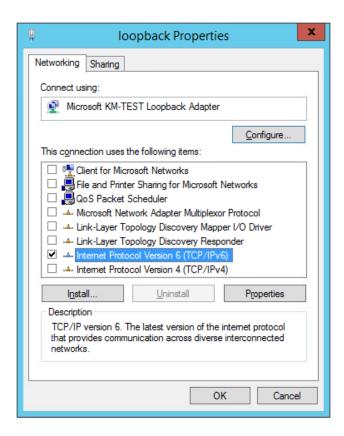


- Note 192.168.2.20 is an example, make sure you specify the correct VIP address.
- Note If a Real Server is included in multiple DR mode VIPs, an IP address for each VIP must be

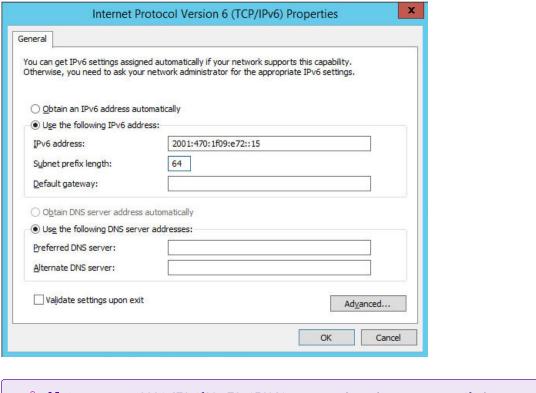
3. Click **OK** then click **Close** to save and apply the new settings.

IPv6 Addresses

1. Uncheck all items except Internet Protocol Version 6 (TCP/IPv6) as shown below:



2. Ensure that Internet Protocol Version (TCP/IPv6) is selected, click Properties and configure the IP address to be the same as the Virtual Service (VIP) and set the Subnet Prefix Length to be the same as your network setting, e.g. 2001:470:1f09:e72::15/64 as shown below:



Note 2001:470:1f09:e72::15/64 is an example, make sure you specify the correct VIP address.

Note
If a Real Server is included in multiple DR mode VIPs, an IP address for each VIP must be added to the Loopback Adapter.

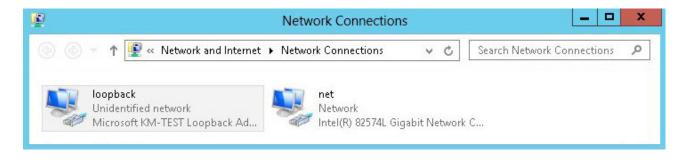
3. Click **OK** then click **Close** to save and apply the new settings.

Step 3 of 3: Configure the strong/weak host behavior

The strong/weak host behavior can be configured using either of the following 2 methods:

- Option 1 Using network shell (netsh) commands
- Option 2 Using PowerShell cmdlets

The commands in this section assume that the LAN Adapter is named "**net**" and the Loopback Adapter is named "**loopback**" as shown in the example below:



Either adjust the commands to use the names allocated to your LAN and loopback adapters, or rename the adapters before running the commands. Names are case sensitive so make sure

that the interface names used in the commands match the adapter names exactly.

Option 1 - Using Network Shell (netsh) Commands

To configure the correct strong/weak host behavior run the following commands:

For IPv4 addresses:

```
netsh interface ipv4 set interface "net" weakhostreceive=enabled
netsh interface ipv4 set interface "loopback" weakhostreceive=enabled
netsh interface ipv4 set interface "loopback" weakhostsend=enabled
```

For IPv6 addresses:

```
netsh interface ipv6 set interface "net" weakhostreceive=enabled
netsh interface ipv6 set interface "loopback" weakhostreceive=enabled
netsh interface ipv6 set interface "loopback" weakhostsend=enabled
netsh interface ipv6 set interface "loopback" dadtransmits=0
```

Option 2 - Using PowerShell Cmdlets

For IPv4 addresses:

```
Set-NetIpInterface -InterfaceAlias loopback -WeakHostReceive enabled -WeakHostSend enabled -DadTransmits 0 -AddressFamily IPv4
```

Set-NetIpInterface -InterfaceAlias net -WeakHostReceive enabled -AddressFamily IPv4

For IPv6 Addresses:

Set-NetIpInterface -InterfaceAlias loopback -WeakHostReceive enabled -WeakHostSend enabled -DadTransmits 0 -AddressFamily IPv6

Set-NetIpInterface -InterfaceAlias net -WeakHostReceive enabled -AddressFamily IPv6

16. Document Revision History

Version	Date	Change	Reason for Change	Changed By
1.0.0	17 April 2018	Initial version		АН
1.0.1	6 December 2018	Added the new "Company Contact Information" page	Required updates	АН
1.2.0	18 September 2019	Multiple updates	Revised load balancing design	RJC
1.2.1	17 January 2020	Updated the health check settings for the Synapse Mobility VIP	To improve the accuracy of the health check	RJC
1.2.2	8 April 2020	Added SSL Termination	Revised load balancing design	IBG
1.2.3	27 July 2020	New title page	Branding update	АН
		Updated Canadian contact details	Change to Canadian contact details	
1.3.0	1 January 2022	Converted the document to AsciiDoc	Move to new documentation system	AH, RJC, ZAC
1.3.1	22 April 2022	Updated SSL related content to reflect latest software version	New software release	RJC
1.3.2	11 May 2022	Updated external health check related content to reflect latest software version	New software release	RJC
1.3.3	28 September 2022	Updated layer 7 VIP and RIP creation screenshots	Reflect changes in the web user interface	АН
1.3.4	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	АН

Version	Date	Change	Reason for Change	Changed By
1.3.5	2 February 2023	Updated screenshots	Branding update	АН
1.3.6	7 March 2023	Removed conclusion section	Updates across all documentation	АН
1.4.0	24 March 2023	New document theme Modified diagram colours	Branding update	AH



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.

