LOADBALANCER

DEPLOYMENT GUIDE

Load Balancing NextGen Connect (Mirth)

Version 1.2.0

Table of Contents

1. About this Guide

This guide details the steps required to configure a load balanced NextGen Connect environment utilizing Loadbalancer.org appliances.

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 for load balancing NextGen Connect. 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

- V8.4.1 and later

ℹ 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. NextGen Connect

- All versions

4. Load Balancing NextGen Connect

NextGen Connect, formerly known as Mirth Connect, is a cross-platform interface engine used in the healthcare industry. It enables the management of information using bi-directional sending of many types of messages. Like an interpreter who translates foreign languages into the one you understand, NextGen Connect Integration Engine translates message standards into the one your system understands. Whenever a "foreign" system sends you a message, NextGen Connect Integration Engine’s integration capabilities expedite the following:

- Filtering – NextGen Connect Integration Engine reads message parameters and passes the message to or stops it on its way to the transformation stage
- Transformation – NextGen Connect Integration Engine converts the incoming message standard to another standard (e.g., HL7 to XML)
- Extraction – NextGen Connect Integration Engine can "pull" data from and "push" data to a database
- Routing – NextGen Connect Integration Engine makes sure messages arrive at their assigned destinations

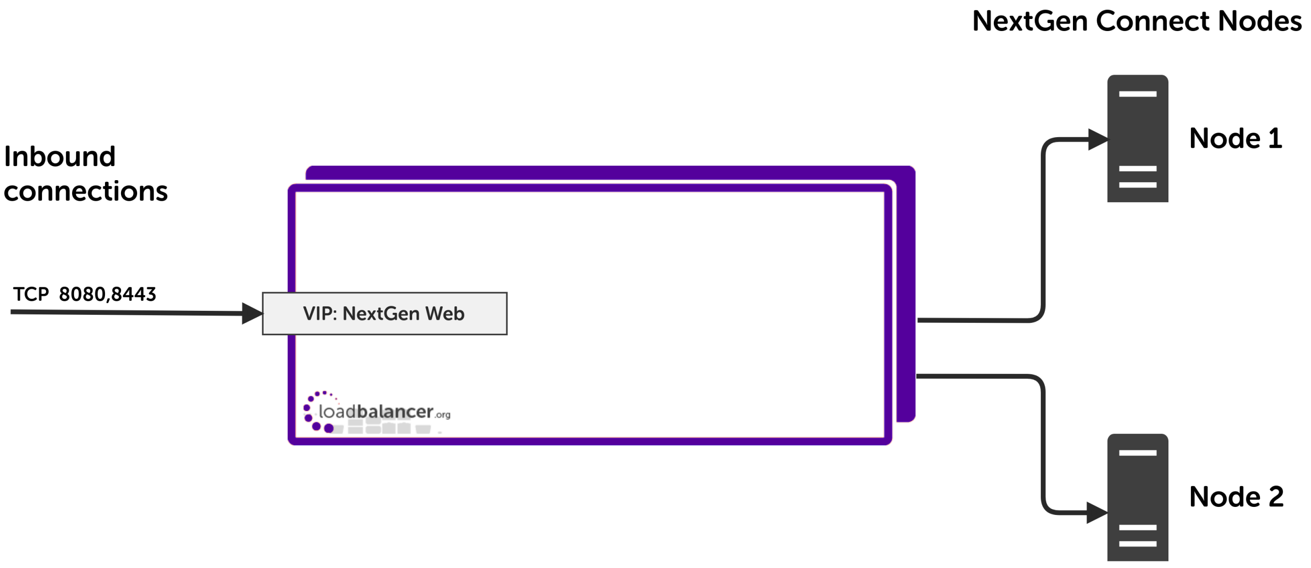
4.1. Ports Requirements

The following table shows the ports used by the NextGen Connect nodes. The load balancer must be configured to listen on the same ports.

Port	Protocols	Use
8080	TCP/HTTP	Web based access to Mirth Connect
8443	TCP/HTTPS	Secure web based access to the Mirth Connect

Load Balancer Deployment

When the NextGen Connect nodes 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 nodes.



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.

4.2. Virtual Service (VIP) Requirements

To provide load balancing for NextGen Connect nodes one VIP is required:

- **VIP 1:** NextGen-HTTP(S)

4.3. Deployment Mode

We recommend using Layer 7 as no network changes are required and SSL termination with re-encryption can be implemented. This mode offers high performance and implementation flexibility, however as Layer 7 is a reverse proxy the client source IP address is not visible at the real server. Instead, the IP address of the load balancer is visible at the real server. In order to retain the client source IP address, the load balancer inserts an *X-Forwarded-For* header into the load balanced traffic, which the NextGen Connect nodes can log for troubleshooting issues while seeing the true source IP address of connecting clients.

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.

ℹ 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.

ℹ 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.

ℹ 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.

ℹ Note	There are certain differences when accessing the WebUI for the cloud appliances. For details, please refer to the relevant Quick Start / Configuration Guide.

ℹ 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/

ℹ Note	You'll receive a warning about the WebUI's certificate. This is due to the default self signed certificate that is used. If preferred, you can upload your own certificate - for more

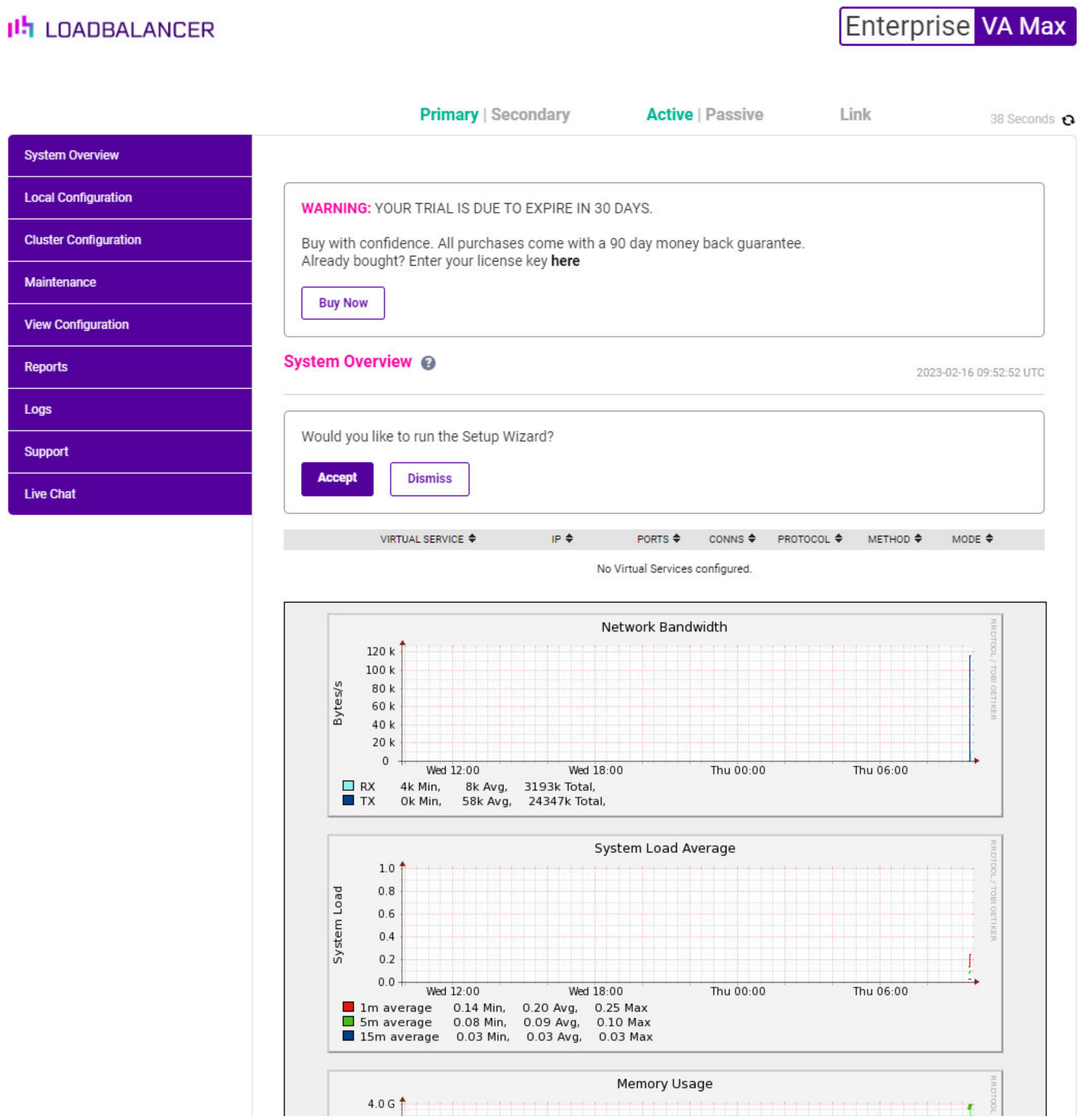
information, please refer to Appliance Security Features.

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

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

ℹ 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

2023-02-16 09:52:52 UTC

Would you like to run the Setup Wizard?

No Virtual Services configured.

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

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

Main Menu Options

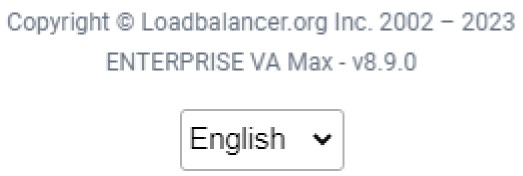
System Overview - Displays a graphical summary of all VIPs, RIPs and key appliance statistics
Local Configuration - Configure local host settings such as IP address, DNS, system time etc.
Cluster Configuration - Configure load balanced services such as VIPs & RIPs
Maintenance - Perform maintenance tasks such as service restarts and taking backups
View Configuration - Display the saved appliance configuration settings
Reports - View various appliance reports & graphs
Logs - View various appliance logs
Support - Create a support download, contact the support team & access useful links
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

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

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

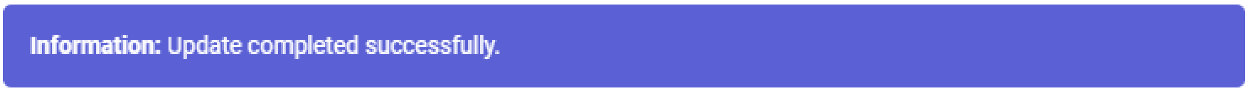
Information: Version v8.9.0 is the current release. No updates are available

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

Note

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

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



Information: Update completed successfully.

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

Using Offline Update

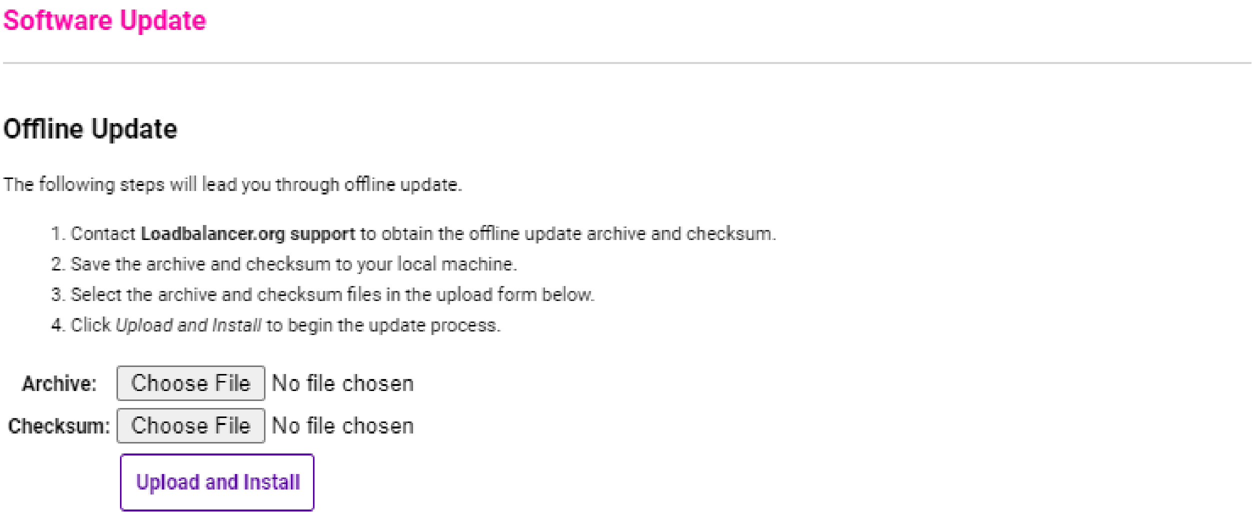
If the load balancer does not have access to the Internet, offline update can be used.

Note

Please contact support@loadbalancer.org 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.

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
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.

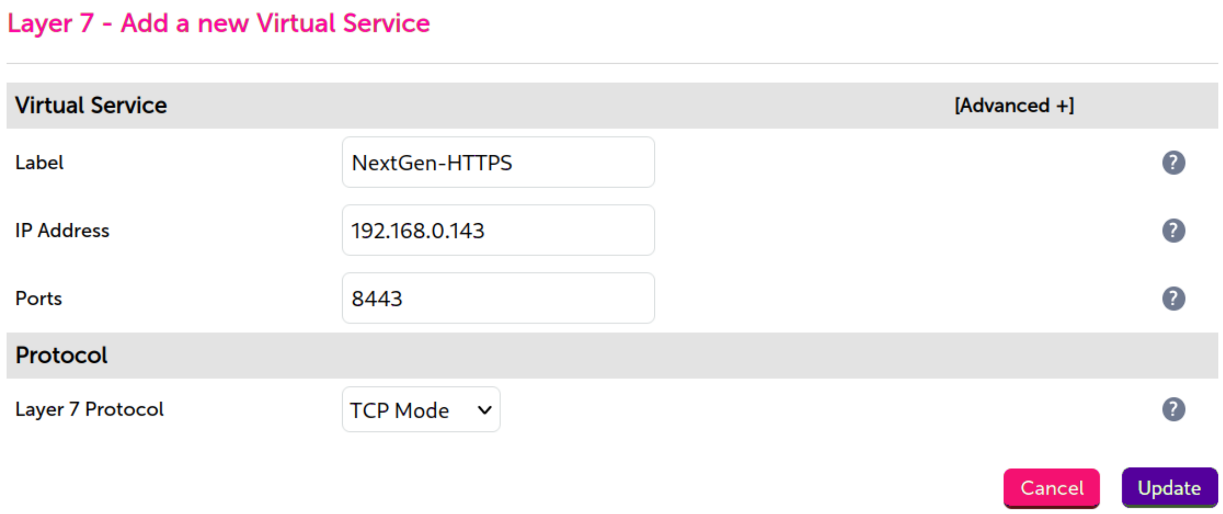
6. Appliance Configuration for NextGen Connect

6.1. Configuring VIP1 – NextGen-HTTPS

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

Virtual Service	[Advanced +]
Label	NextGen-HTTPS
IP Address	192.168.0.143
Ports	8443

Protocol	
Layer 7 Protocol	TCP Mode

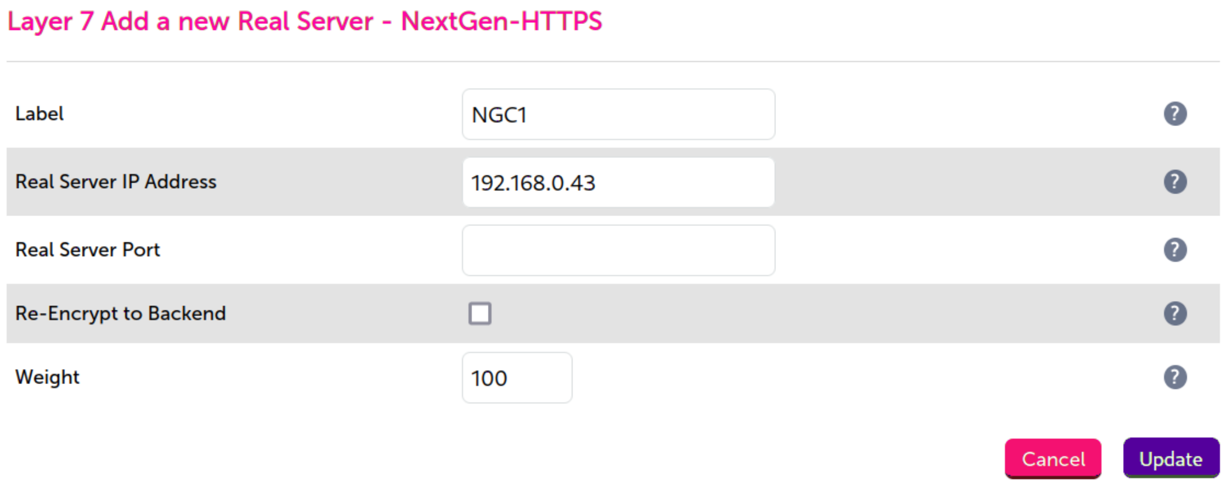
3. Enter an appropriate label (name) for the VIP, e.g. **NextGen-HTTPS**.

4. Set the *Virtual Service IP* address field to the required IP address, e.g. **192.168.0.143**.

5. Set the *Virtual Service Ports* field to **8443**.
6. Set *Protocol* to **TCP Mode**.
7. Click **Update**.
8. Click **Modify** next to the newly created VIP.
9. Set *Persistence Mode* to **Source IP**.
10. Set *Health Checks* to **Negotiate HTTPS (HEAD)**.
11. Under the *Other* section click ***Advanced***.
12. Under *Timeout* check the box.
13. Set the *Client Timeout* and *Real Server Timeout* to **5m**.
14. Click **Update**.

b) Setting up the 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 NextGen-HTTPS VIP.
2. Enter the following details:



Layer 7 Add a new Real Server - NextGen-HTTPS

Label	NGC1
Real Server IP Address	192.168.0.43
Real Server Port	
Re-Encrypt to Backend	☐
Weight	100

3. Enter an appropriate label (name) for the RIP, e.g. **NGC1**.
4. Set the *Real Server IP Address* field to the IP address of the NextGen Connect node, e.g. **192.168.0.43**.
5. Click **Update**.
6. Repeat these steps to add additional NextGen Connect nodes as real servers as required.

6.2. Finalizing the Configuration

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

1. Using the WebUI, navigate to: *Maintenance > Restart Services*.

2. Click **Reload HAProxy**.

7. Additional Configuration Options & Settings

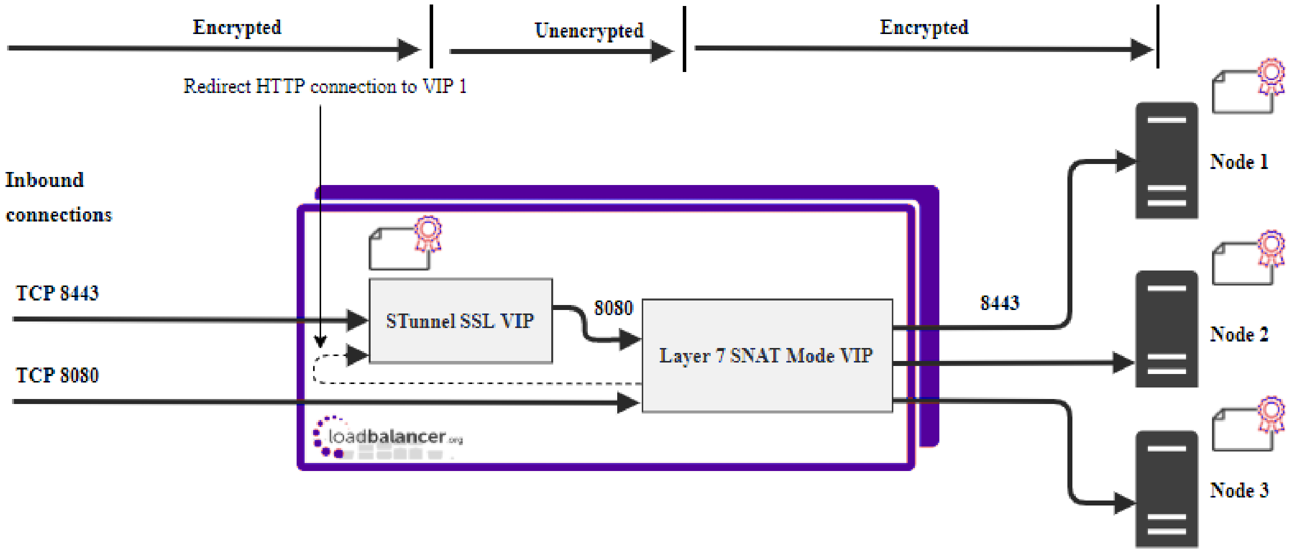
7.1. SSL Termination

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**.

> ℹ Note
>
> SSL termination on the load balancer can be very CPU intensive.
>
> 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 mode VIP. Layer 4 DR mode cannot be used since stunnel acts as a proxy, and the NextGen Connect node servers see requests with a source IP address of the VIP. However, since the NextGen Connect 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.
>
> In the context of a NextGen Connect deployment *only **SSL Bridging** is an accepted configuration*.
>
> ***Force to HTTPS*** is not compatible with NextGen Connect nodes and therefore should be disabled.

7.2. SSL Termination on the load balancer - SSL Bridging



In this case an STunnel SSL Virtual Service is defined 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 and is also encrypted from the load balancer to the backend servers as shown above.

Certificates

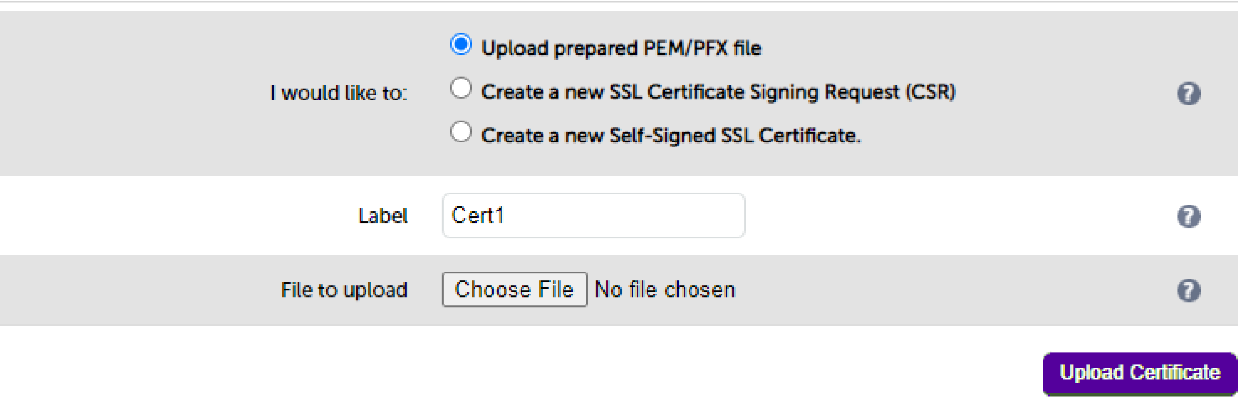
If you already have an SSL certificate in either PFX or PEM file format, this can be uploaded to the Load balancer using the certificate upload option as explained below in Uploading Certificates. Alternatively, you can create a Certificate Signing Request (CSR) on the load balancer and send this to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

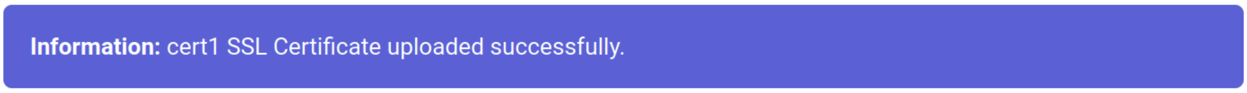


I would like to: ● Upload prepared PEM/PFX file ○ Create a new SSL Certificate Signing Request (CSR) ○ Create a new Self-Signed SSL Certificate.

Label: Cert1

File to upload: Choose File No file chosen

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.

> **Note** It's important to back up all of your certificates. This can be done via the WebUI from *Maintenance > Backup & Restore > Download SSL Certificates.*

7.3. Configuring SSL Termination on the Load Balancer

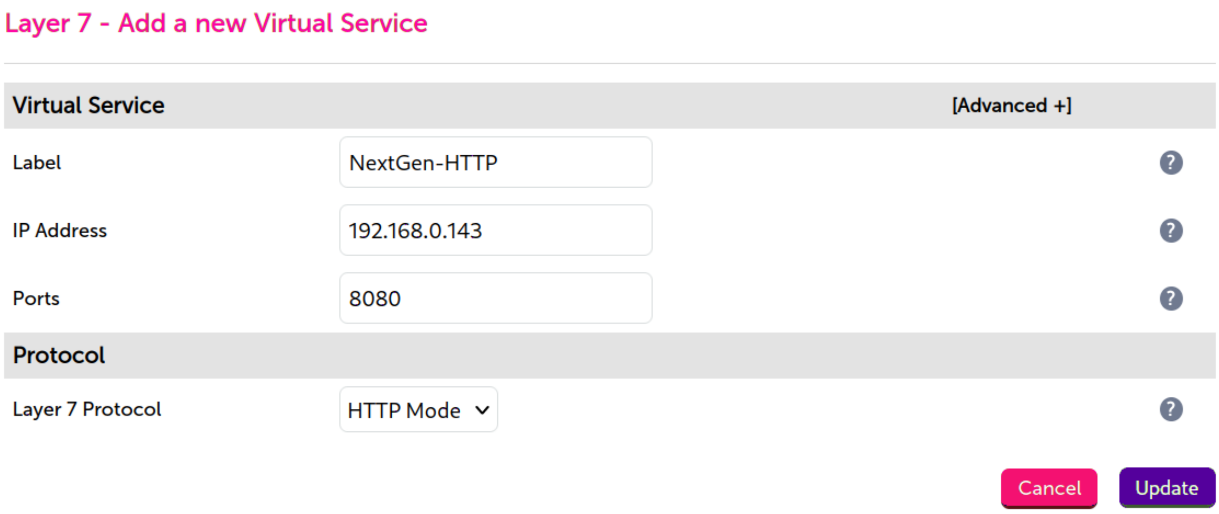
To configure SSL termination for NextGen:

1. Configure a layer 7 HTTP mode VIP to handle HTTP traffic
2. Configure SSL termination to handle HTTPS traffic

7.4. 1) Configuring 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:



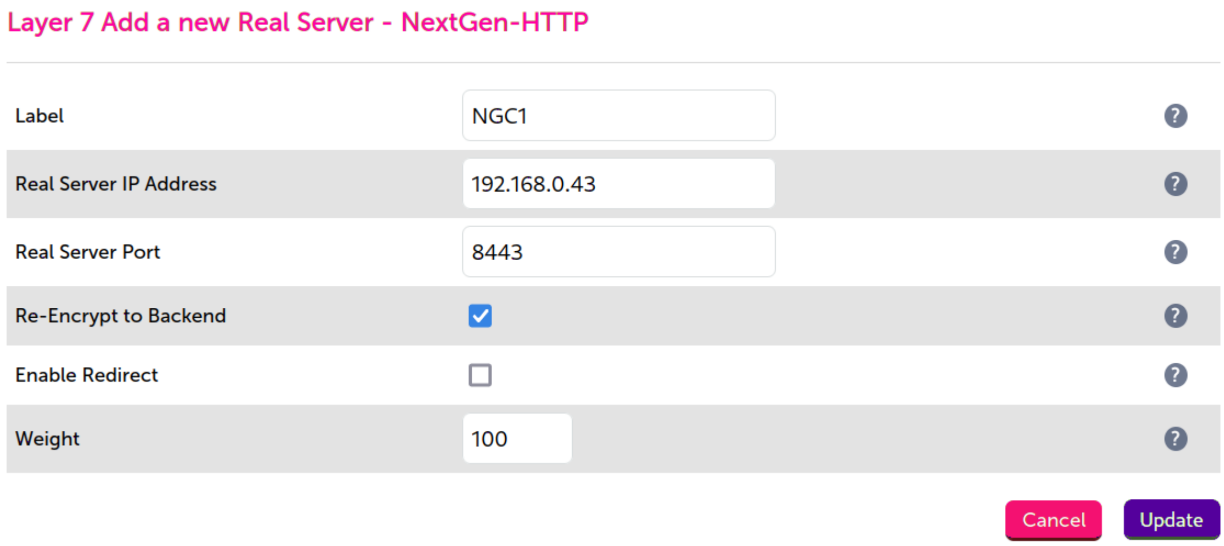
Layer 7 - Add a new Virtual Service

Virtual Service	[Advanced +]
Label	NextGen-HTTP
IP Address	192.168.0.143
Ports	8080
Protocol	
Layer 7 Protocol	HTTP Mode

3. Enter an appropriate label (name) for the VIP, e.g. **NextGen-HTTP**.
4. Set the *Virtual Service IP* address field to the required IP address, e.g. **192.168.0.200**.
5. Set the *Virtual Service Ports* field to **8080**.
6. Leave *Protocol* set to **HTTP Mode**.
7. Click **Update**.
8. Click **Modify** next to the newly created VIP.
9. Set *Persistence Mode* to **HTTP Cookie and Source IP**.
10. Set *Health Checks* to **Negotiate HTTPS (HEAD)**.
11. Click **Advanced**.
12. Set *Check Port* to **8443**.
13. Under *SSL* check **Enable Backend Encryption**.
14. Under the *Other* section click ***Advanced***.
15. Under *Timeout* check the box.
16. Set the *Client Timeout* and *Real Server Timeout* to **5m**.
17. Click **Update**.

b) Setting up the 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 NextGen-HTTP VIP.
2. Enter the following details:



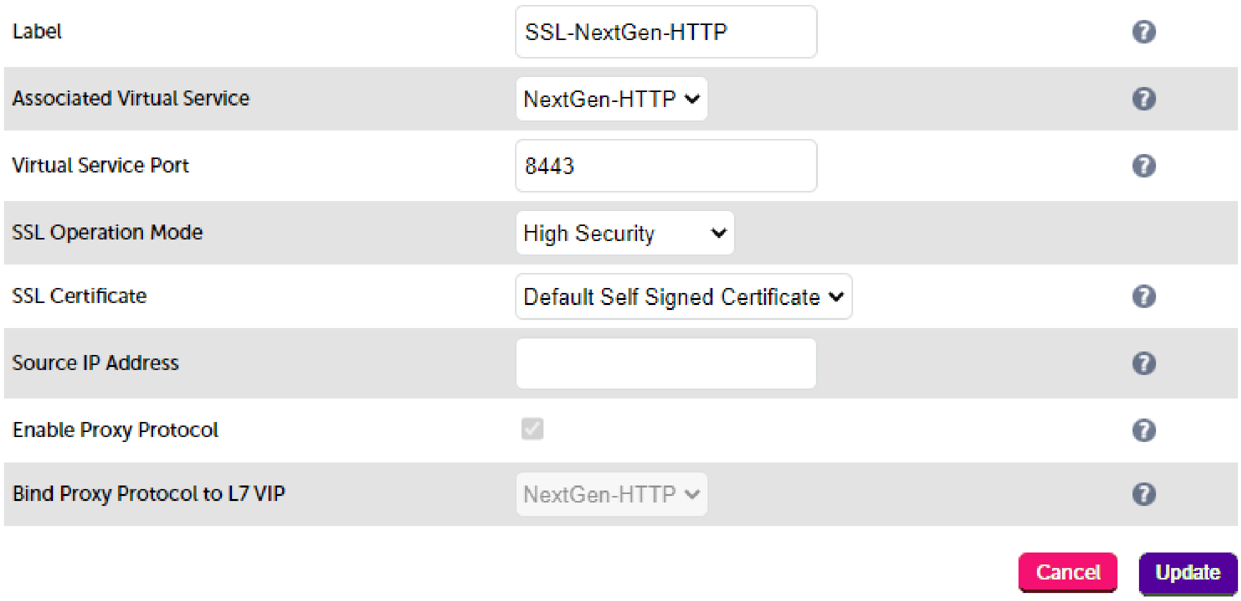
Layer 7 Add a new Real Server - NextGen-HTTP

Label	NGC1
Real Server IP Address	192.168.0.43
Real Server Port	8443
Re-Encrypt to Backend	☑
Enable Redirect	□
Weight	100

3. Enter an appropriate label (name) for the RIP, e.g. **NGC1**.
4. Set the *Real Server IP Address* field to the IP address of the NextGen Connect node.
5. Click **Update**.
6. Repeat these steps to add additional NextGen Connect nodes as real servers as required.

7.5. 2) Configure SSL termination

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



Label	SSL-NextGen-HTTP
Associated Virtual Service	NextGen-HTTP
Virtual Service Port	8443
SSL Operation Mode	High Security
SSL Certificate	Default Self Signed Certificate
Source IP Address	
Enable Proxy Protocol	☑
Bind Proxy Protocol to L7 VIP	NextGen-HTTP

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

> ℹ 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 the use of the HTTP Cookie and Source IP persistence method. The connection is then re-encrypted and forwarded to the real server.

7.6. 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:

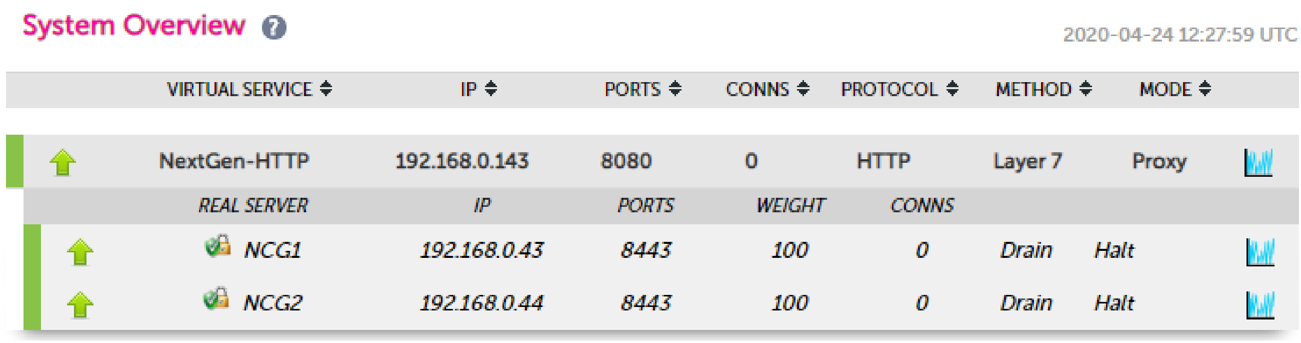
1. Using the WebUI, navigate to: *Maintenance > Restart Services*.
2. Click **Reload HAProxy**.
3. Click **Reload STunnel**.

8. Testing & Verification

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

8.1. Using System Overview

The System Overview can be viewed in the WebUI. It shows a graphical view of all VIPs & RIPs (i.e. NextGen-HTTP) 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 NextGen Connect nodes are healthy and available to accept connections.



System Overview

2020-04-24 12:27:59 UTC

VIRTUAL SERVICE	IP	PORTS	CONNS	PROTOCOL	METHOD	MODE
NextGen-HTTP	192.168.0.143	8080	0	HTTP	Layer 7	Proxy
REAL SERVER	*IP*	*PORTS*	*WEIGHT*	*CONNS*		
NCG1	*192.168.0.43*	*8443*	*100*	*0*	*Drain*	*Halt*
NCG2	*192.168.0.44*	*8443*	*100*	*0*	*Drain*	*Halt*

9. 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.

10. Further Documentation

For additional information, please refer to the Administration Manual.

11. Appendix

11.1. 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.

> **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:

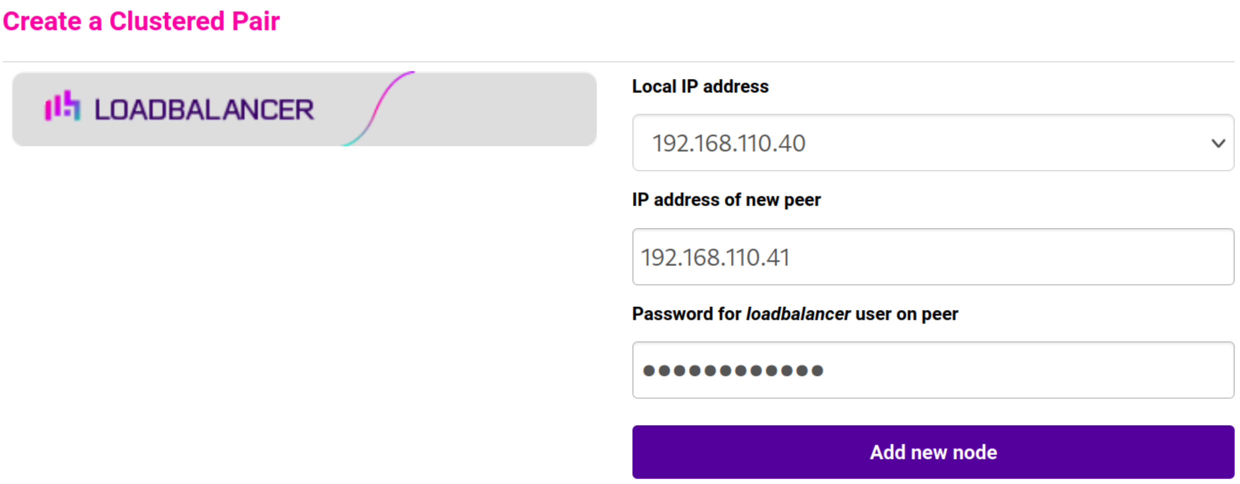
WebUI Main Menu Option	Sub Menu Option	Description
Local Configuration	Hostname & DNS	Hostname and DNS settings
Local Configuration	Network Interface Configuration	All network settings including IP address(es), bonding configuration and VLANs
Local Configuration	Routing	Routing configuration including 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

> 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*.



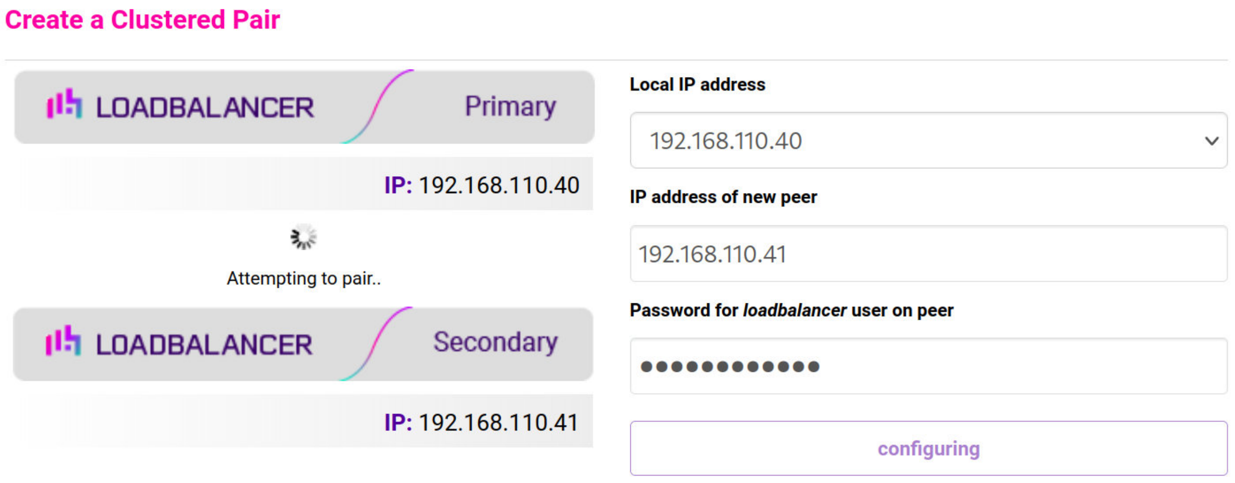
Create a Clustered Pair

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

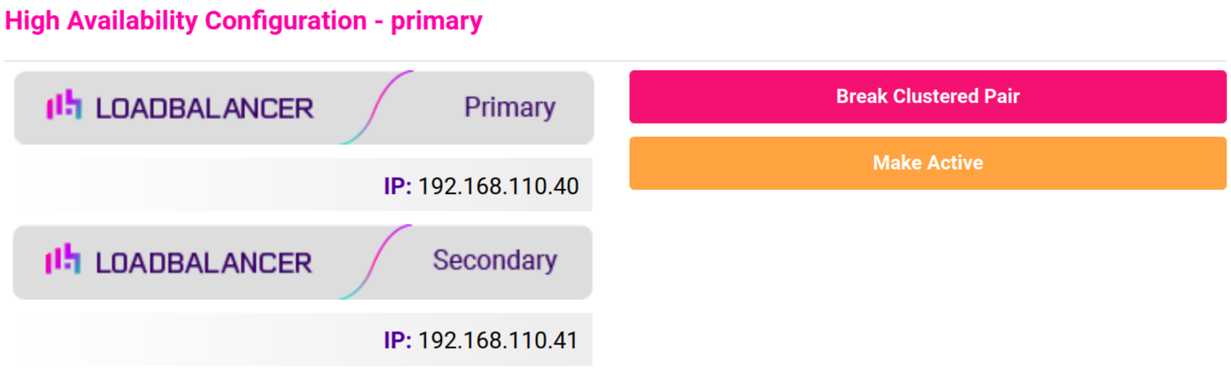
Attempting to pair..

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

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.

12. Document Revision History

Version	Date	Change	Reason for Change	Changed By
1.0.0	24 April 2020	Initial document creation		IBG
1.0.1	1 September 2020	New title page Updated Canadian contact details	Branding update Change to Canadian contact details	AH
1.1.0	1 January 2022	Converted the document to AsciiDoc	Move to new documentation system	AH, RJC, ZAC
1.1.1	26 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

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.