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 relevant Administration Manual:

- v7 Administration Manual
- v8 Administration Manual

2. Loadbalancer.org Appliances Supported

The complete list of our products that are supported for load balancing NextGen Connect is shown below:

<table>
<thead>
<tr>
<th>Discontinued Models</th>
<th>Current Models *</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enterprise R16</td>
<td>Enterprise R20</td>
</tr>
<tr>
<td>Enterprise VA R16</td>
<td>Enterprise MAX</td>
</tr>
<tr>
<td>Enterprise VA</td>
<td>Enterprise 10G</td>
</tr>
<tr>
<td></td>
<td>Enterprise 40G</td>
</tr>
<tr>
<td></td>
<td>Enterprise Ultra</td>
</tr>
<tr>
<td></td>
<td>Enterprise VA R20</td>
</tr>
<tr>
<td></td>
<td>Enterprise VA MAX</td>
</tr>
</tbody>
</table>

* For full specifications of these models please refer to: [http://www.loadbalancer.org/products/hardware](http://www.loadbalancer.org/products/hardware)

3. Loadbalancer.org Software Versions Supported

- V8.4.1 and later

4. NextGen Connect Software Versions Supported

- NextGen Connect – all versions
5. 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.

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.

<table>
<thead>
<tr>
<th>Port</th>
<th>Protocols</th>
<th>Use</th>
</tr>
</thead>
<tbody>
<tr>
<td>8080</td>
<td>TCP/HTTP</td>
<td>Web based access to Mirth Connect</td>
</tr>
<tr>
<td>8443</td>
<td>TCP/HTTPS</td>
<td>Secure web based access to the Mirth Connect</td>
</tr>
</tbody>
</table>
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 section 1 in the appendix on page 18 for more details on configuring a clustered pair.

Virtual Service (VIP) Requirements

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

- VIP 1: NextGen-HTTP(S)

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.
6. Loadbalancer.org Appliance – the Basics

Virtual Appliance Download & Deployment
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 and XEN and has been optimized for each Hypervisor. By default, the VA is allocated 1 CPU, 2GB of RAM and has an 8GB 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 the Administration Manual and the ReadMe.txt text file included in the VA download for more detailed information on deploying the VA using various Hypervisors.

Initial Network Configuration
The IP address, subnet mask, default gateway and DNS settings can be configured in several ways as detailed below:

**Method 1 – Using the Network Setup Wizard at the console**
After boot up, follow the instructions on the console to configure the IP address, subnet mask, default gateway and DNS settings.

**Method 2 – Using the WebUI**
Using a browser, connect to the WebUI on the default IP address/port: [https://192.168.2.21:9443](https://192.168.2.21:9443)
To set the IP address & subnet mask, use: *Local Configuration > Network Interface Configuration*
To set the default gateway, use: *Local Configuration > Routing*
To configure DNS settings, use: *Local Configuration > Hostname & DNS*

Accessing the Web User Interface (WebUI)

1. Browse to the following URL: [https://192.168.2.21:9443/lbadmin/](https://192.168.2.21:9443/lbadmin/)
   (replace with your IP address if it's been changed)
   *Note the port number → 9443*
2. Login to the WebUI:

**Username:** loadbalancer  
**Password:** loadbalancer

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

Once logged in, the WebUI will be displayed as shown below:
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 slave unit is covered in section 1 of the appendix on page 18.
7. Appliance & NextGen Connect Node Configuration

Appliance Configuration

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](image)

   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](image)

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

8. Additional Configuration Options & Settings

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

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 Local SSL 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.

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 on page 12. Alternatively, you can create a Certificate Signing Request (CSR) and send this to your CA to create a new certificate.

Generating a CSR on the Load Balancer

CSR’s can be generated on the load balancer to apply for a certificate from your chosen CA.

To generate a CSR:

1. Using the WebUI, navigate to: Cluster Configuration > SSL Certificates
2. Click Add a new SSL Certificate & select Create a New SSL Certificate (CSR)
3. Enter a suitable label (name) for the certificate, e.g. Cert1
4. Populate the remaining fields according to your requirements
5. Once all fields are complete click Create CSR
6. To view the CSR click Modify next to the new certificate, then expand the Certificate Signing Request (CSR) section
7. Copy the CSR and send this to your chosen CA
8. Once received, copy/paste your signed certificate into the Your Certificate section
9. Intermediate and root certificates can be copied/pasted into the Intermediate Certificate and Root Certificate sections as required
10. Click Update to complete the process

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:

   ![Image]

   **Information:** cert1 SSL Certificate uploaded successfully

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

**Configuring SSL Termination on the Load Balancer**

To configure an SSL VIP the steps are outlined below:

1. Configure a layer 7 HTTP mode VIP
2. Configure SSL termination with re-encrypt to the backend

**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:
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 the 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:
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

2) Configure SSL termination

For v8.3.3 and later:
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. 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.
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 the 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
7. Click Reload STunnel when prompted to apply the new settings using the button provided in the blue box

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.

Finalizing the Configuration
To apply the new settings, HAProxy must be reloaded as follows:

1. Using the WebUI, navigate to: Maintenance > Restart Services and click Reload HAProxy
9. Testing & Verification

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.

10. 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.

11. Further Documentation


12. Conclusion

Loadbalancer.org appliances provide a very cost effective solution for highly available load balanced NextGen Connect environments.
13. Appendix

1 – Clustered Pair Configuration – Adding a Slave Unit
If you initially configured just the master unit and now need to add a slave - our recommended procedure, please refer to the relevant section below for more details:

Note: A number of settings are not replicated as part of the master/slave pairing process and therefore must be manually configured on the slave appliance. These are listed below:

- Hostname & DNS settings
- Network settings including IP addresses, bonding configuration and VLANs
- Routing configuration including default gateways and static routes
- Date & time settings
- Physical – Advanced Configuration settings including Internet Proxy IP address & port, Firewall table size, SMTP relay and Syslog server
- SNMP settings
- Graphing settings
- Firewall Script & Firewall Lockdown Script settings
- Software updates

Version 7:
Please refer to Chapter 8 – Appliance Clustering for HA in the v7 Administration Manual.

Version 8:
To add a slave node – i.e. create a highly available clustered pair:
1. Deploy a second appliance that will be the slave and configure initial network settings
2. Using the WebUI, navigate to: *Cluster Configuration > High-Availability Configuration*
   Specify the IP address and the *loadbalancer* users password (the default is 'loadbalancer') for the slave (peer) appliance as shown above

3. Click **Add new node**

![Create a Clustered Pair](image)

4. The pairing process now commences as shown below:

![High Availability Configuration - Master](image)

5. Once complete, the following will be displayed:

![High Availability Configuration - Master](image)

6. To finalize the configuration, restart heartbeat and any other services as prompted in the blue message box at the top of the screen

   **Note:** Clicking the **Restart Heartbeat** button on the master appliance will also automatically restart heartbeat on the slave appliance.

   **Note:** Please refer to chapter 9 – Appliance Clustering for HA in the Administration Manual for more detailed information on configuring HA with 2 appliances.
## 14. Document Revision History

<table>
<thead>
<tr>
<th>Version</th>
<th>Date</th>
<th>Change</th>
<th>Reason for Change</th>
<th>Changed By</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.0.0</td>
<td>24 April 2020</td>
<td>Initial document creation</td>
<td></td>
<td>IBG</td>
</tr>
<tr>
<td>1.0.1</td>
<td>1 September 2020</td>
<td>New title page</td>
<td>Branding update</td>
<td>AH</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Updated Canadian contact</td>
<td>Change to Canadian contact details</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>details</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
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.

United Kingdom
Loadbalancer.org Ltd.
Compass House, North Harbour Business Park, Portsmouth, PO6 4PS
UK:+44 (0) 330 380 1064
sales@loadbalancer.org
support@loadbalancer.org

Canada
Loadbalancer.org Appliances Ltd.
300-422 Richards Street, Vancouver, BC, V6B 2Z4, Canada
TEL:+1 866 998 0508
sales@loadbalancer.org
support@loadbalancer.org

United States
Loadbalancer.org, Inc.
4550 Linden Hill Road, Suite 201
Wilmington, DE 19808, USA
TEL: +1 833.274.2566
sales@loadbalancer.org
support@loadbalancer.org

Germany
Loadbalancer.org GmbH
Tengstraße 2780798,
München, Germany
TEL: +49 (0)89 2000 2179
sales@loadbalancer.org
support@loadbalancer.org