LOADBALANCER

DEPLOYMENT GUIDE

Load Balancing Kofax AutoStore

Version 1.3.0

Table of Contents

1. About this Guide

This guide details the steps required to configure a load balanced Kofax AutoStore environment utilizing Loadbalancer.org appliances. It covers the configuration of the load balancers and also any Kofax AutoStore 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 for load balancing Kofax AutoStore. For full specifications of available models please refer to https://www.loadbalancer.org/products.

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

3. Software Versions Supported

3.1. Loadbalancer.org Appliance

- V8.9.1 and later

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

3.2. Kofax AutoStore

- Version 7.0

4. Kofax AutoStore

AutoStore is a server based middle-tier application that captures, processes, and routes paper and electronic documents in a business environment. It lowers costs and improves operational efficiency for organizations of all sizes by automating document handling processes.

AutoStore provides a flexible component-based server for capturing electronic and paper documents. Some of AutoStore's capabilities include:

- 'Capture components' to capture documents from scanners and multifunction devices, fax, email, smartphones and tablets, XML data streams, PC desktops, office applications, and network and FTP locations
- 'Process components' to support functionalities to detect, read, extract, store, convert, classify, and index content in captured documents

- 'Route components' to deliver documents to virtually any destination such as fax, email, network folders, PCs, and document management systems

5. Load Balancing Kofax AutoStore

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

5.1. Load Balancing & HA Requirements

In order to be successfully load balanced, a Kofax AutoStore deployment must feature the following components:

- Wide Area Network (WAN)
- Local Area Network (LAN)
- Firewall
- SQL Server
- Web Server
- Active Directory
- File Share

It is likely that a fully functional AutoStore deployment will already feature all of these components.

5.2. Persistence (aka Server Affinity)

MFDs from some vendors require source IP address persistence to be used for the AutoStore servers. This ensures that a particular client will connect to the same AutoStore server for the duration of the session.

MFDs from some vendors do not require session affinity at the load balancing layer.

Specific persistence settings for some of the most common vendors are described in the application configuration instructions later in this guide.

5.3. Virtual Service (VIP) Requirements

To provide load balancing and HA for AutoStore, a single VIP is required. The traffic that is load balanced and the ports that are used vary between vendors. Specific settings for some of the most common vendors are described in the application configuration instructions later in this guide.

5.4. Port Requirements

The following tables show the ports that are load balanced for four of the most common vendors:

Xerox EIP Connect

Port	Protocols	Use
3241	TCP	Capture server port

Konica Minolta

Port	Protocols	Use
3348	TCP/HTTP	AutoStore Web Server
13351	TCP/HTTP	OpenAPI Application
13353	TCP/HTTPS	OpenAPI Authority
13391	TCP/HTTP	WebDAV Session

Ricoh ESA

Port	Protocols	Use
8084	TCP	Capture
8753	TCP	DRS

Ricoh SOP

Port	Protocols	Use
3350	TCP	Capture
8753	TCP	DRS

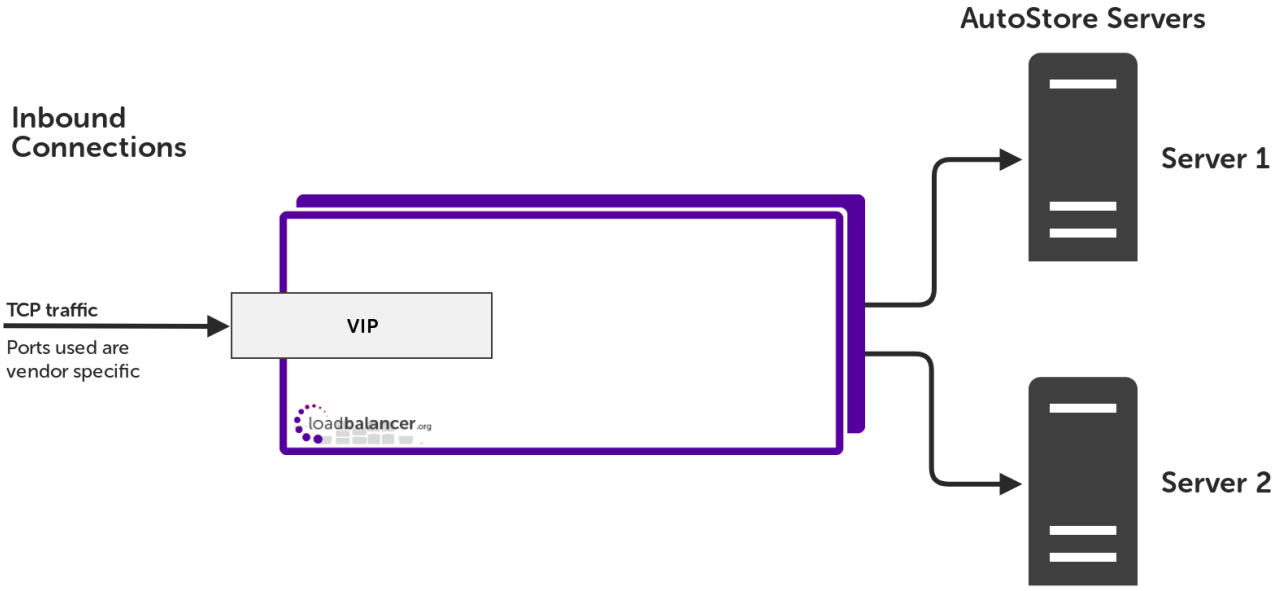
Other Vendors

If using a vendor that is not listed above, please follow the following hyperlink and refer to the port list for AutoStore provided by Kofax:

https://knowledge.kofax.com/MFD_Productivity/AutoStore/Configuration/AutoStore_7_Default_ports_for_capture_process_and_route_components

The list includes the web application port / capture server port / web server port that should be used for a variety of vendors and services.

6. Deployment Concept



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

> **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.

7. Load Balancer Deployment Methods

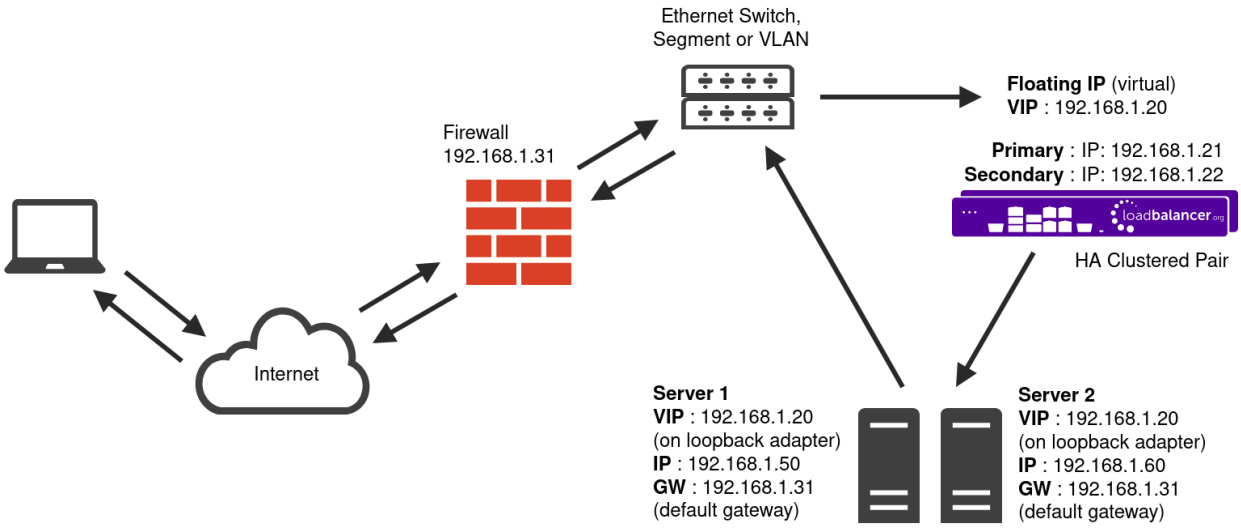
The load balancer can be deployed in either *Layer 4 DR mode or Layer 4 NAT mode*.

For Kofax AutoStore, layer 4 DR mode is recommended unless a two arm configuration is needed. These modes are described below and are used for the configurations presented in this guide. For configuring using DR mode please refer to Appliance Configuration for Kofax AutoStore – Using Layer 4 DR Mode, and for configuring using layer 4 NAT mode refer to Appliance Configuration for Kofax AutoStore – Using Layer 4 NAT Mode.

7.1. Layer 4 DR Mode

Layer 4 DR (Direct Routing) mode is a very high performance solution that requires little change to your existing infrastructure.

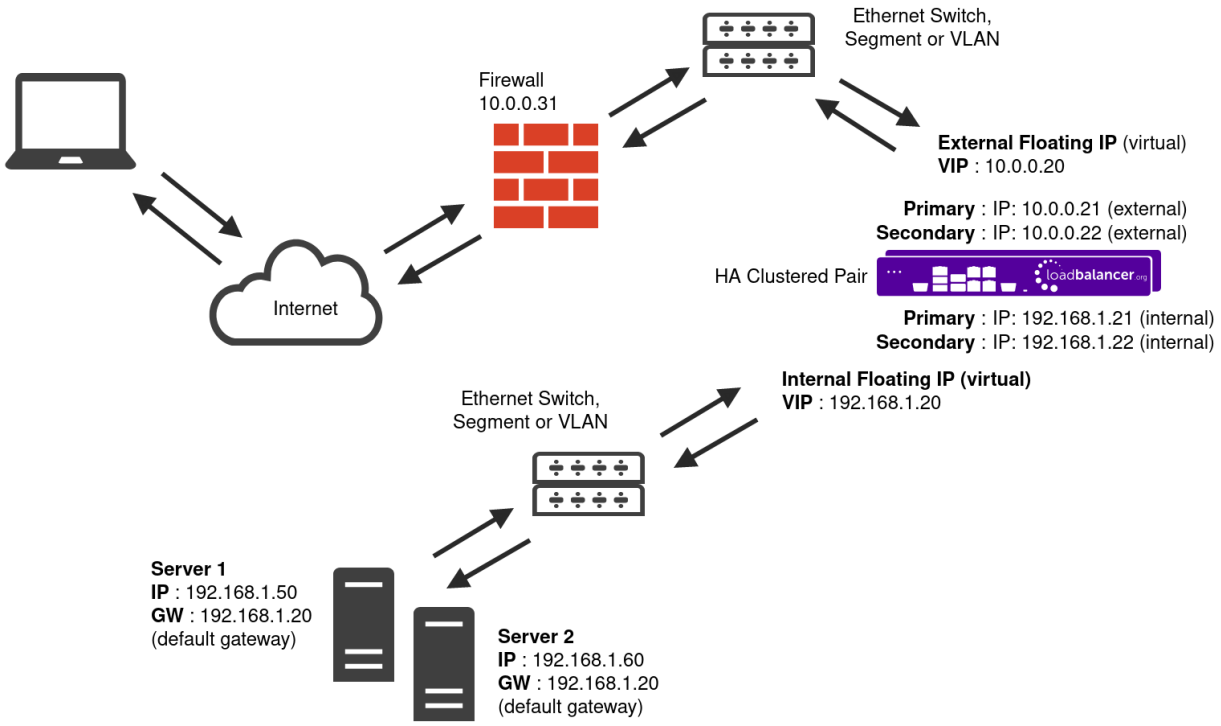
> **Note** Kemp, Brocade, Barracuda & A10 Networks call this *Direct Server Return* and F5 call it *nPath*.



- DR mode works by changing the destination MAC address of the incoming packet to match the selected Real Server on the fly which is very fast.
- When the packet reaches the Real Server it expects the Real Server to own the Virtual Services IP address (VIP). This means that each Real Server (and the load balanced application) must respond to both the Real Server's own IP address and the VIP.
- The Real Server should not respond to ARP requests for the VIP. Only the load balancer should do this. Configuring the Real Server in this way is referred to as "Solving the ARP Problem". For more information please refer to DR Mode Considerations.
- On average, DR mode is 8 times quicker than NAT mode for HTTP and much faster for other applications such as Remote Desktop Services, streaming media and FTP.
- The load balancer must have an interface in the same subnet as the Real Servers to ensure layer 2 connectivity which is required for DR mode to operate.
- The VIP can be brought up on the same subnet as the Real Servers or on a different subnet provided that the load balancer has an interface in that subnet.
- Port translation is not possible with DR mode, e.g. VIP:80 → RIP:8080 is not supported.
- DR mode is transparent, i.e. the Real Server will see the source IP address of the client.

7.2. Layer 4 NAT Mode

Layer 4 NAT mode is a high performance solution, although not as fast as layer 4 DR mode. This is because real server responses must flow back to the client via the load balancer rather than directly as with DR mode.



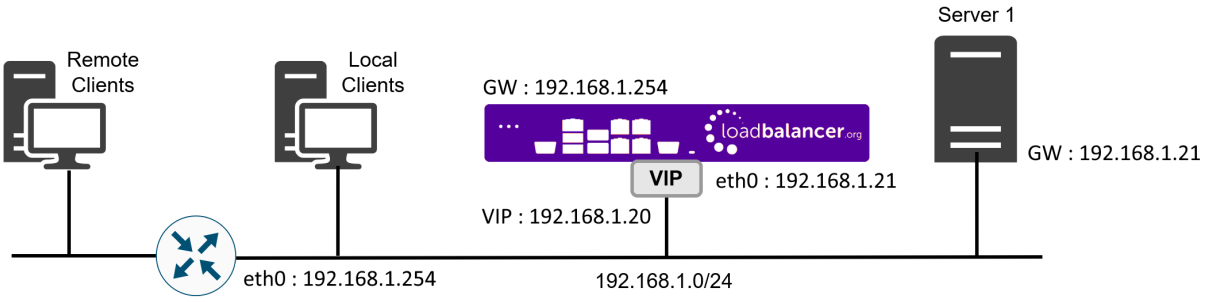
- The load balancer translates all requests from the Virtual Service to the Real Servers.
- NAT mode can be deployed in the following ways:
  - **Two-arm (using 2 Interfaces)** (as shown above) - Here, 2 subnets are used. The VIP is located in one subnet and the load balanced Real Servers are located in the other. The load balancer requires 2 interfaces, one in each subnet.

> **Note** This can be achieved by using two network adapters, or by creating VLANs on a single adapter.

    - Normally **eth0** is used for the internal network and **eth1** is used for the external network although this is optional. Any interface can be used for any purpose.
    - If the Real Servers require Internet access, *Auto-NAT* should be enabled using the WebUI menu option: *Cluster Configuration > Layer 4 - Advanced Configuration*, the external interface should be selected.
    - The default gateway on the Real Servers must be set to be an IP address on the load balancer.

> **Note** For an HA clustered pair, a floating IP should be added to the load balancer and used as the Real Server's default gateway. This ensures that the IP address can "float" (move) between Primary and Secondary appliances.

    - Clients can be located in the same subnet as the VIP or any remote subnet provided they can route to the VIP.
  - **One-arm (using 1 Interface)** - Here, the VIP is brought up in the same subnet as the Real Servers.



- To support remote clients, the default gateway on the Real Servers must be an IP address on the load balancer and routing on the load balancer must be configured so that return traffic is routed back via the router.

> **Note** For an HA clustered pair, a floating IP should be added to the load balancer and used as the Real Server's default gateway. This ensures that the IP address can "float" (move) between Primary and Secondary appliances.

- To support local clients, return traffic would normally be sent directly to the client bypassing the load balancer which would break NAT mode. To address this, the routing table on the Real Servers must be modified to force return traffic to go via the load balancer. For more information please refer to One-Arm (Single Subnet) NAT Mode.

- If you want Real Servers to be accessible on their own IP address for non-load balanced services, e.g. RDP, you will need to setup individual SNAT and DNAT firewall script rules for each Real Server or add additional VIPs for this.
- Port translation is possible with Layer 4 NAT mode, e.g. VIP:80 → RIP:8080 is supported.
- NAT mode is transparent, i.e. the Real Server will see the source IP address of the client.

NAT Mode Packet re-Writing

In NAT mode, the inbound destination IP address is changed by the load balancer from the Virtual Service IP address (VIP) to the Real Server. For outbound replies the load balancer changes the source IP address of the Real Server to be the Virtual Services IP address.

The following table shows an example NAT mode setup:

Protocol	VIP	Port	RIP	Port
TCP	10.0.0.20	80	192.168.1.50	80

In this simple example all traffic destined for IP address 10.0.0.20 on port 80 is load-balanced to the real IP address 192.168.1.50 on port 80.

Packet rewriting works as follows:

1) The incoming packet for the web server has source and destination addresses as:

Source	x.x.x.x:34567	**Destination**	10.0.0.20:80

2) The packet is rewritten and forwarded to the backend server as:

Source	x.x.x.x:34567	**Destination**	192.168.1.50:80

3) Replies return to the load balancer as:

Source	192.168.1.50:80	**Destination**	x.x.x.x:34567

4) The packet is written back to the VIP address and returned to the client as:

Source	10.0.0.20:80	**Destination**	x.x.x.x:34567

7.3. Our Recommendation

Where possible we recommend that Layer 4 Direct Routing (DR) mode is used. This mode offers the best possible performance since replies go directly from the Real Servers to the client, not via the load balancer. It's also relatively simple to implement. Ultimately, the final choice does depend on your specific requirements and infrastructure.

If DR mode cannot be used, for example if it is required to use a 2-arm configuration, then layer 4 NAT mode is recommended.

8. Configuring Kofax AutoStore for Load Balancing

8.1. Device Registration Service Configuration

Kofax AutoStore needs to be configured via the Device Registration Service (DRS) so that it is highly available and can be load balanced.

The information for the load balanced virtual service needs to be entered into the DRS in the ***Add Application*** section.

- Set an appropriate name, e.g. **xerox**.
- Select the appropriate *Application Type* from the drop-down list, e.g. **Xerox EIP Connect**.
- Set the *AutoStore Server Address* to the virtual IP (VIP) address that will be used for the AutoStore virtual service.
- Set the *Print Manager Address* to the VIP used for the Output Manager backend.
- Set the *Web Application Port* as needed, depending on the MFD vendor:
  - For Xerox EIP Connect, use port **3241**
  - For Konica Minolta, use port **3348**
  - For Ricoh ESA, use port **8084**

- For Ricoh SOP, use port **3350**
- For other vendors, refer to Other Vendors

> **Note** If any configuration changes are made to the AutoStore real servers they will need to be unregistered and then re-registered in the Device Registration Service for the configurations to be accepted.

> **Note** Multi-function devices (MFDs) should be in the same group/folder in the Device Registration Service so that they inherit the same configuration.

8.2. Layer 4 DR Mode – Solving the ARP Problem

If using layer 4 DR mode, the 'ARP problem' must be solved on each real server for DR mode to work. For detailed steps on solving the ARP problem for Windows, please refer to Solving the ARP Problem for more information.

For a detailed explanation of DR mode and the nature of the ARP problem, please refer to Layer 4 DR Mode.

9. Loadbalancer.org Appliance – the Basics

9.1. Virtual Appliance

A fully featured, fully supported 30 day trial is available if you are conducting a PoC (Proof of Concept) deployment. The VA is currently available for VMware, Virtual Box, Hyper-V, KVM, XEN and Nutanix AHV and has been optimized for each Hypervisor. By default, the VA is allocated 2 vCPUs, 4GB of RAM and has a 20GB virtual disk. The Virtual Appliance can be downloaded here.

> **Note** The same download is used for the licensed product, the only difference is that a license key file (supplied by our sales team when the product is purchased) must be applied using the appliance's WebUI.

> **Note** Please refer to Virtual Appliance Installation and the ReadMe.txt text file included in the VA download for additional information on deploying the VA using the various Hypervisors.

> **Note** The VA has 4 network adapters. For VMware only the first adapter (**eth0**) is connected by

default. For HyperV, KVM, XEN and Nutanix AHV all adapters are disconnected by default. Use the network configuration screen within the Hypervisor to connect the required adapters.

9.2. Initial Network Configuration

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

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

9.3. Accessing the Appliance WebUI

The WebUI is accessed using a web browser. By default, users are authenticated using Apache authentication. Users can also be authenticated against LDAP, LDAPS, Active Directory or Radius - for more information, please refer to External Authentication.

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

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

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

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

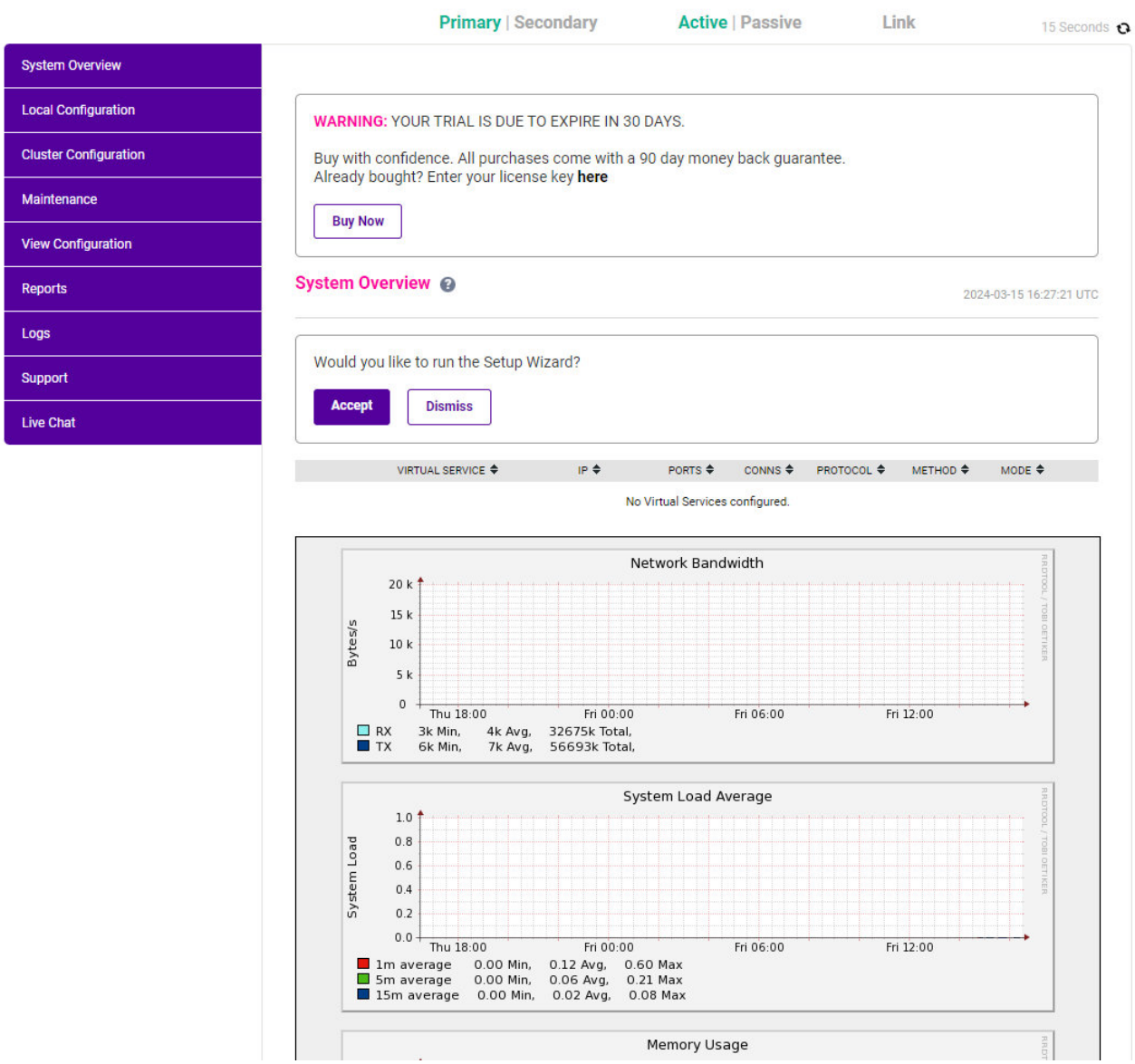
   > **Note** If you need to change the port, IP address or protocol that the WebUI listens on, please refer to Service Socket Addresses.

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

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

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

   Once logged in, the WebUI will be displayed as shown below:



3. You'll be asked if you want to run the Setup Wizard which can be used to configure layer 7 services. Click **Dismiss** if you're following a guide or want to configure the appliance manually or click **Accept** to start the wizard.

Main Menu Options

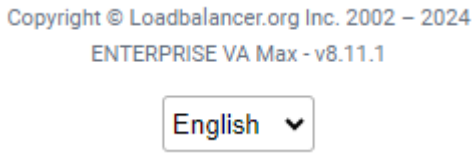
System Overview - Displays a graphical summary of all VIPs, RIPs and key appliance statistics
Local Configuration - Configure local host settings such as IP address, DNS, system time etc.
Cluster Configuration - Configure load balanced services such as VIPs & RIPs
Maintenance - Perform maintenance tasks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

9.4. 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

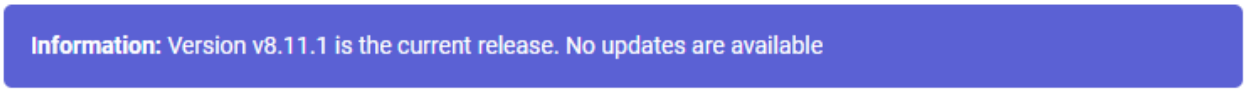
The software version is displayed at the bottom of the WebUI as shown in the example below:



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:



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:

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

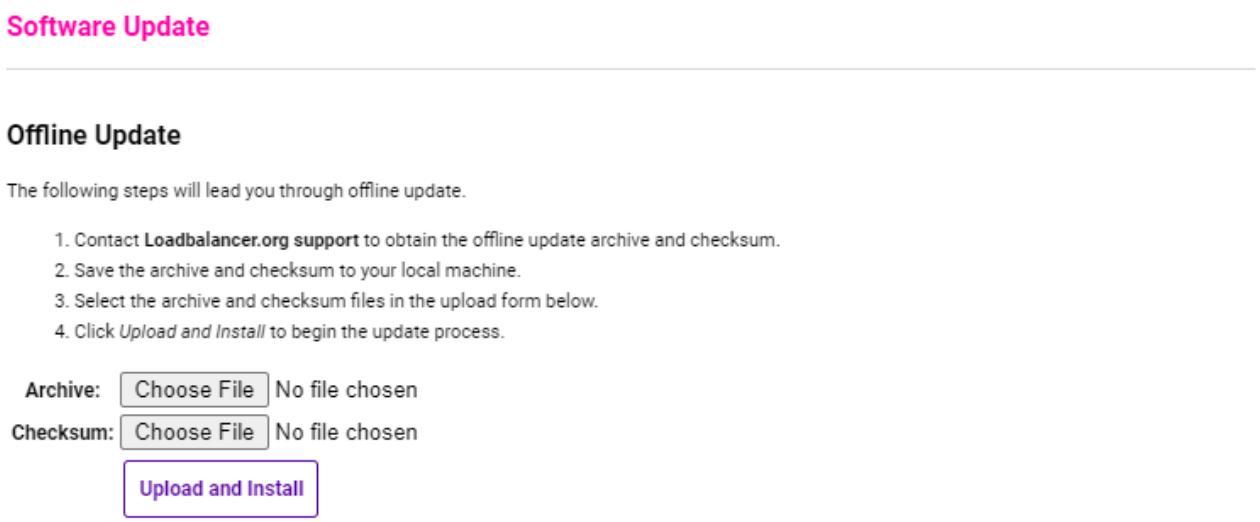
Using Offline Update

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:



4. Select the *Archive* and *Checksum* files.
5. Click **Upload and Install**.
6. If services need to be reloaded/restarted or the appliance needs a full restart, you'll be prompted accordingly.

9.5. Ports Used by the Appliance

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

Protocol	Port	Purpose
TCP	22 *	SSH
TCP & UDP	53 *	DNS / GSLB
TCP & UDP	123	NTP
TCP & UDP	161 *	SNMP
UDP	6694	Heartbeat between Primary & Secondary appliances in HA mode
TCP	7778	HAProxy persistence table replication
TCP	9000 *	Gateway service (Centralized/Portal Management)
TCP	9080 *	WebUI - HTTP (disabled by default)
TCP	9081 *	Nginx fallback page

Protocol	Port	Purpose
TCP	9443 *	WebUI - HTTPS
TCP	25565 *	Shuttle service (Centralized/Portal Management)

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

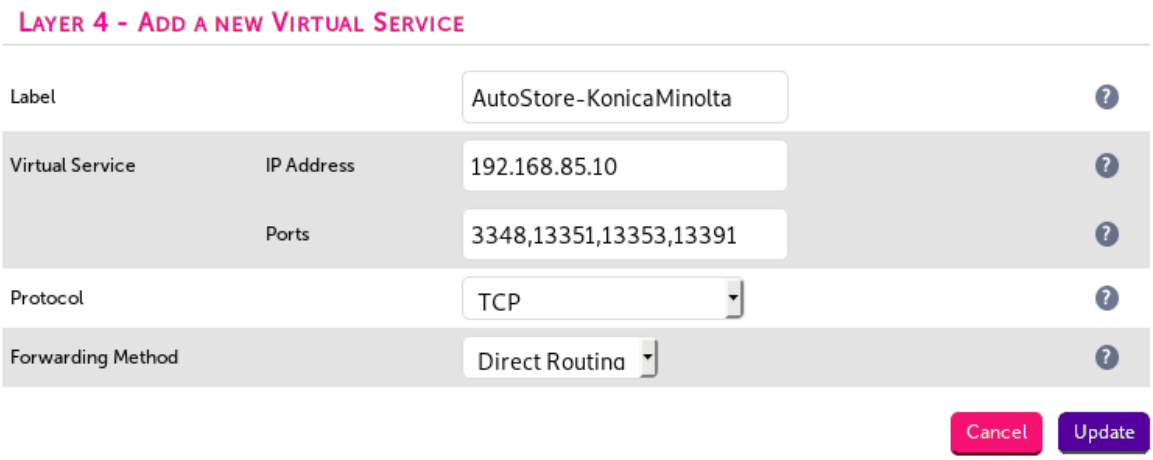
9.6. HA Clustered Pair Configuration

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

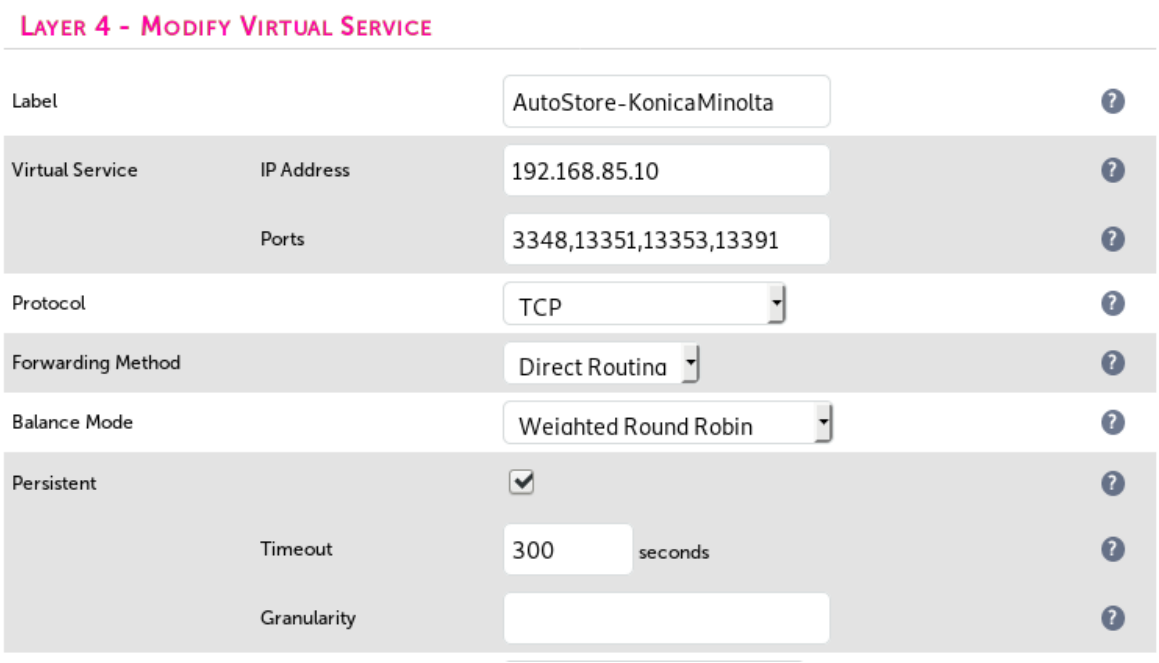
10. Appliance Configuration for Kofax AutoStore – Using Layer 4 DR Mode

10.1. Configuring the Virtual Service (VIP)

1. Using the web user interface, navigate to *Cluster Configuration > Layer 4– Virtual Services* and click on **Add a new Virtual Service**.
2. Define the *Label* for the virtual service as required, e.g. **AutoStore-KonicaMinolta**.
3. Set the *Virtual Service IP Address* field to the required IP address, e.g. **192.168.85.10**.
4. Set the *Ports* field as needed, as a comma separated list, depending on the MFD vendor:
   - For Xerox EIP Connect, use port **3241**
   - For Konica Minolta, use ports **3348**, **13351**, **13353**, and **13391**
   - For Ricoh ESA, use ports **8084** and **8753**
   - For Ricoh SOP, use ports **3350** and **8753**
   - For other vendors, refer to Other Vendors
5. Leave the *Protocol* set to **TCP**.
6. Leave the *Forwarding Method* set to **Direct Routing**.
7. Click **Update** to create the virtual service.



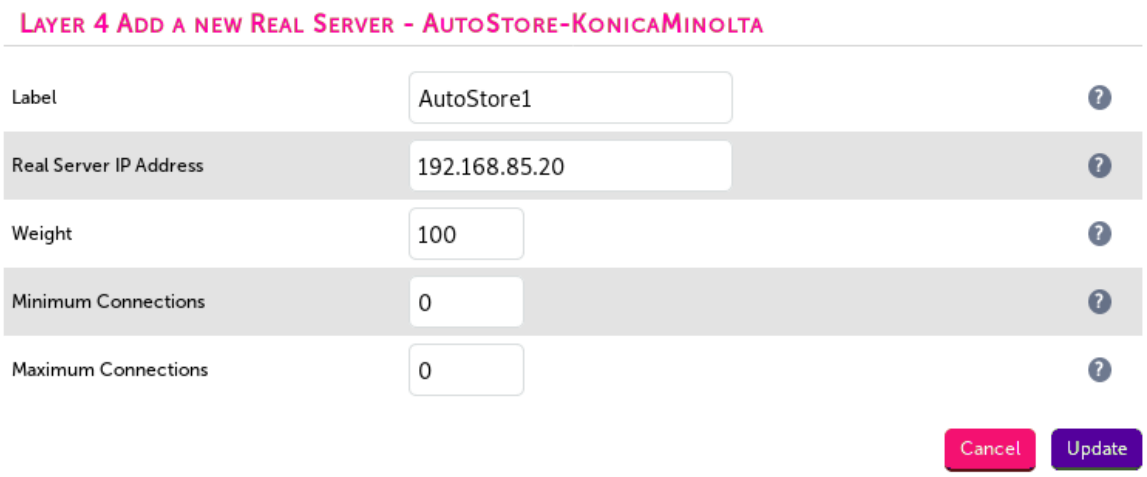
8. Click **Modify** next to the newly created VIP.
9. Set *Balance Mode* to **Weighted Round Robin**.
10. Set the persistence settings as required, depending on the MFD vendor:
    - For Xerox EIP Connect and Konica Minolta:
      - Make sure that the *Persistent* checkbox is checked
      - Set the *Timeout* value to **300** (the units are seconds)
    - For Ricoh ESA and Ricoh SOP, make sure that the *Persistent* checkbox is not selected
11. Click **Update**.



10.2. Defining the Real Servers (RIPs)

1. Using the web user interface, navigate to *Cluster Configuration > Layer 4 – Real Servers* and click on **Add a new Real Server** next to the newly created VIP.
2. Define the *Label* for the real server as required, e.g. **AutoStore1**.

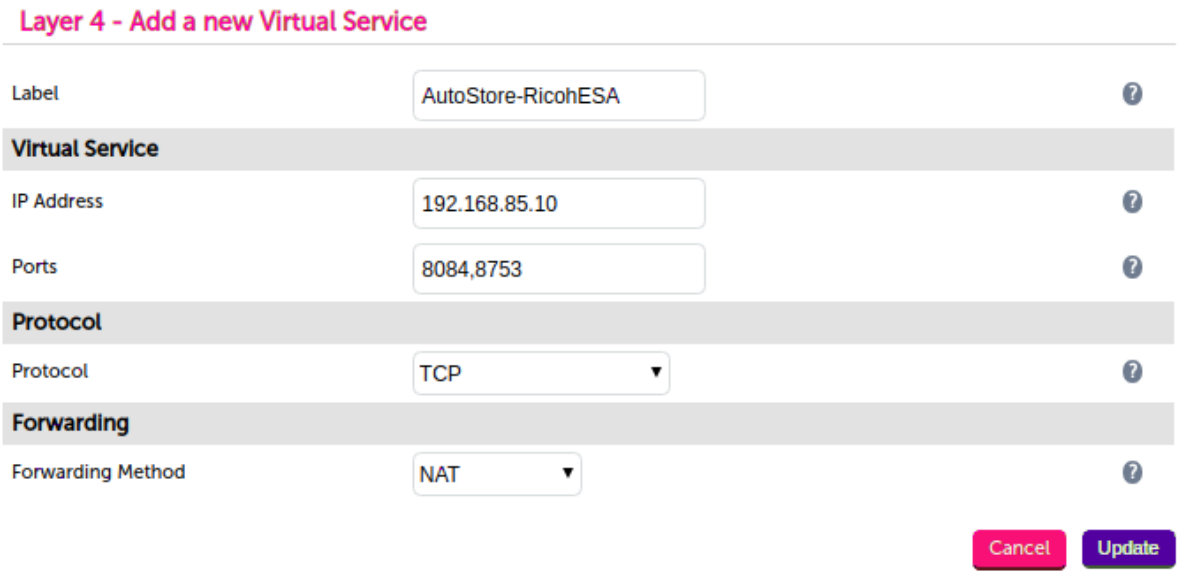
3. Set the *Real Server IP Address* field to the required IP address, e.g. **192.168.85.20**.
4. Click **Update**.
5. Repeat these steps to add additional AutoStore servers as required.



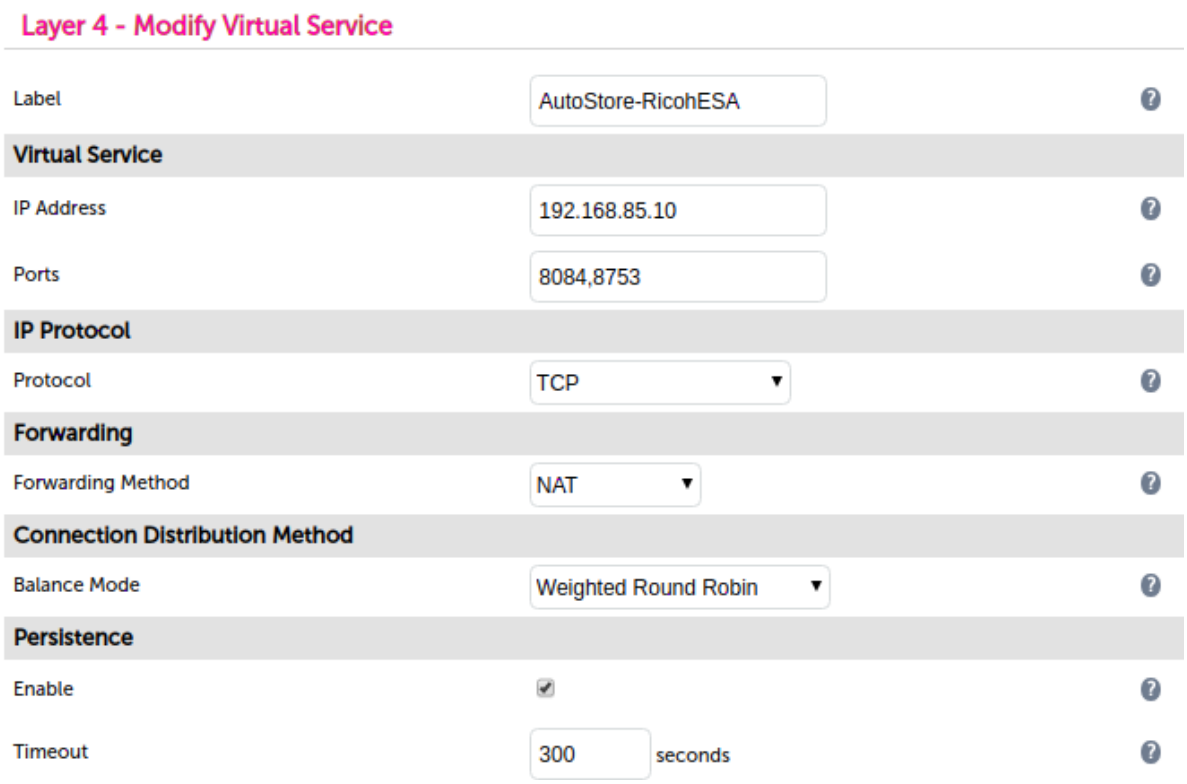
11. Appliance Configuration for Kofax AutoStore – Using Layer 4 NAT Mode

11.1. Configuring the Virtual Service (VIP)

1. Using the web user interface, navigate to *Cluster Configuration > Layer 4 – Virtual Services* and click on **Add a new Virtual Service**.
2. Enter an appropriate name for the VIP in the *Label* field, e.g. **AutoStore-RicohESA**.
3. Set the *Virtual Service IP* address field to the required IP address, e.g. **192.168.85.10**.
4. Set the *Virtual Service Ports* field as needed, as a comma separated list, depending on the MFD vendor:
   - For Xerox EIP Connect, use port **3241**
   - For Konica Minolta, use ports **3348**, **13351**, **13353**, and **13391**
   - For Ricoh ESA, use ports **8084** and **8753**
   - For Ricoh SOP, use ports **3350** and **8753**
   - For other vendors, refer to Other Vendors
5. Set the *Forwarding Method* to **NAT**.

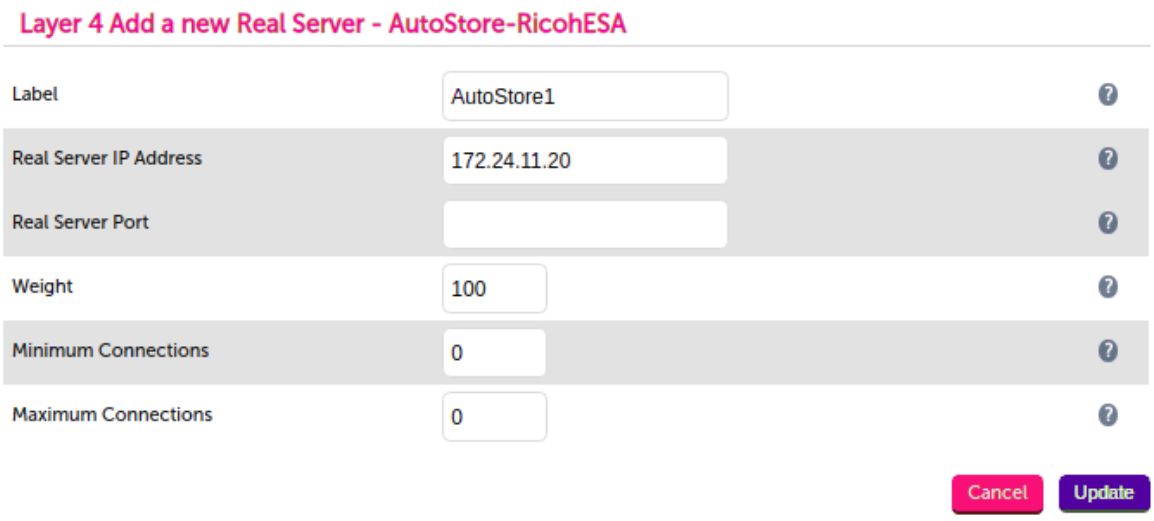


6. Click **Update** to create the virtual service.
7. Click **Modify** next to the newly created VIP.
8. Set *Balance Mode* to **Weighted Round Robin**.
9. Set the *Persistence Mode* settings as required, depending on the MFD vendor:
    - For Xerox EIP Connect and Konica Minolta:
        - Set *Persistence Mode* to **Source IP** persistence
        - Set the *Timeout* value to **300** (the units are seconds)
    - For Ricoh ESA and Ricoh SOP, set *Persistence Mode* to **None**
10. Click **Update**.



11.2. Defining the Real Servers (RIPs)

1. Using the web user interface, navigate to *Cluster Configuration > Layer 4 – Real Servers* and click on **Add a new Real Server** next to the newly created VIP.
2. Enter an appropriate name for the server in the *Label* field, e.g. **AutoStore1**.
3. Change the *Real Server IP Address* field to the required IP address, e.g. **172.24.11.20**.
4. Leave the *Real Server Port* field empty.
5. Click **Update**.
6. Repeat these steps to add additional AutoStore servers as required.



12. Testing & Verification

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

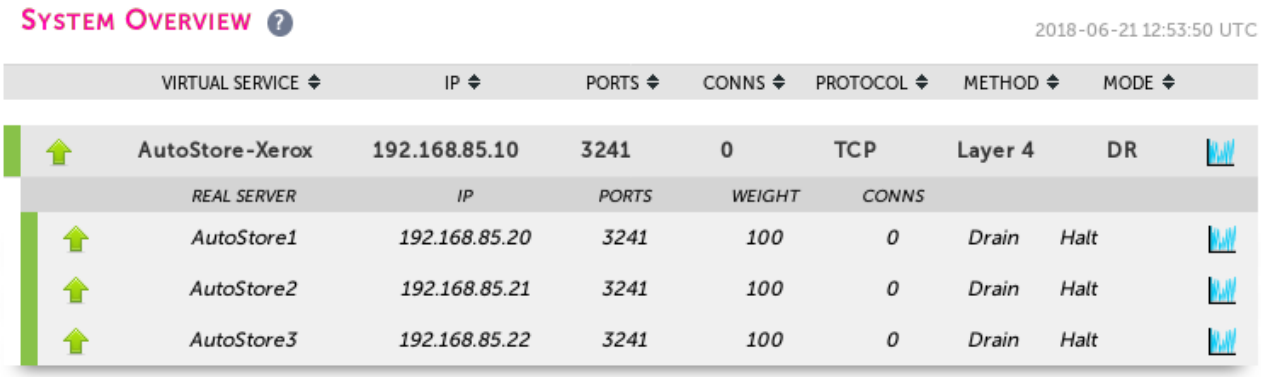
12.1. Testing Using a Multi-function Device

Once all configuration is complete on the AutoStore servers, in the Device Registration Service, and on the load balancer, it is possible to test the new load balanced service using a multi-function device.

1. Authenticate at a configured multi-function device.
2. Press the Kofax button and then select a scan template, for example to scan to home or scan to e-mail.
3. Set the scan options as appropriate, and complete a test scan.
4. AutoStore should recognise the user authenticated at the multi-function device and then route the test scan as requested. Verify that the test scan arrives at its intended destination.

12.2. Using System Overview

The System Overview can be viewed in the WebUI. It shows a graphical view of all VIPs & RIPs (i.e. the AutoStore 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 AutoStore servers are healthy and available to accept connections.



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. Further Documentation

For additional information, please refer to the Administration Manual.

15. Appendix

15.1. Solving the ARP Problem

Windows Server 2012 & Later

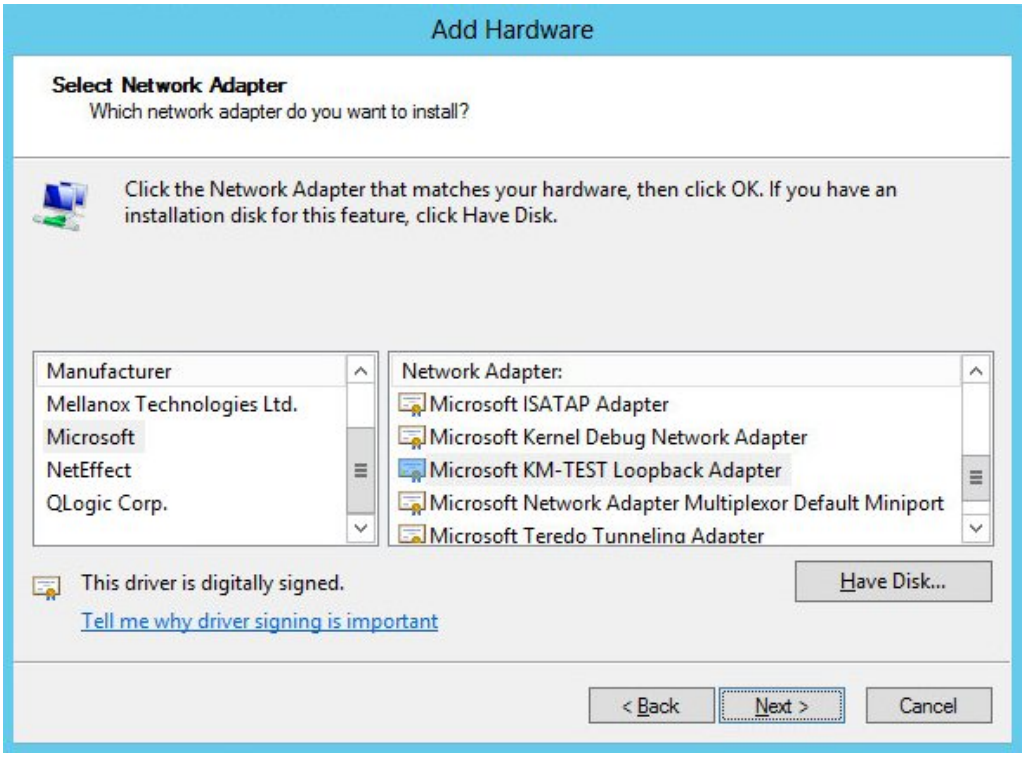
Windows Server 2012 and later support Direct Routing (DR) mode through the use of the Microsoft Loopback Adapter that must be installed and configured on each load balanced (Real) Server. The IP address configured on the Loopback Adapter must be the same as the Virtual Service (VIP) address. This enables 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, the strong/weak host behavior must be configured on each Real Server. The weak host model allows packets with any IP to be sent or received via an interface. The strong host model only allows packets with an IP belonging to the interface to be sent or received.

> **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

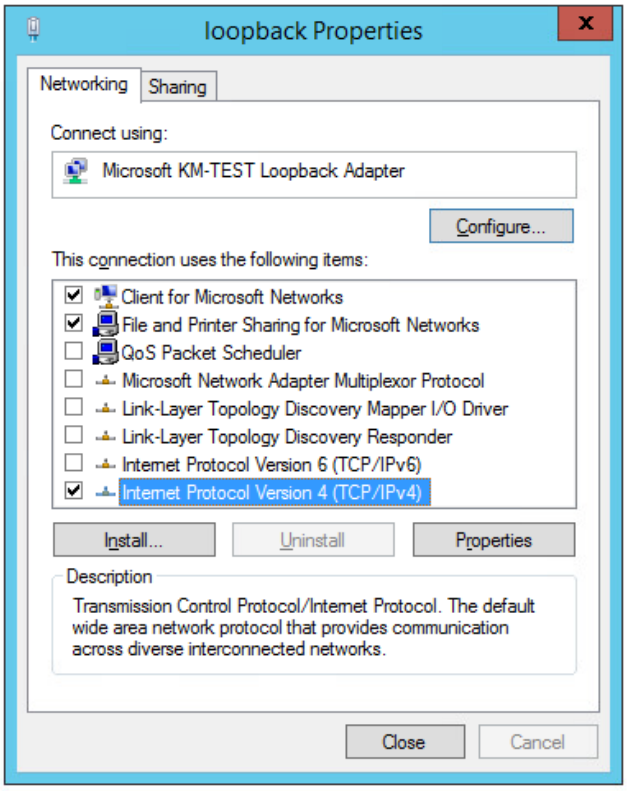
1. Open Control Panel and click **Network and Sharing Center**.
2. Click **Change adapter settings**.
3. Right-click the new Loopback Adapter and select **Properties**.

> **Note** You can configure IPv4 or IPv6 addresses or both depending on your requirements.

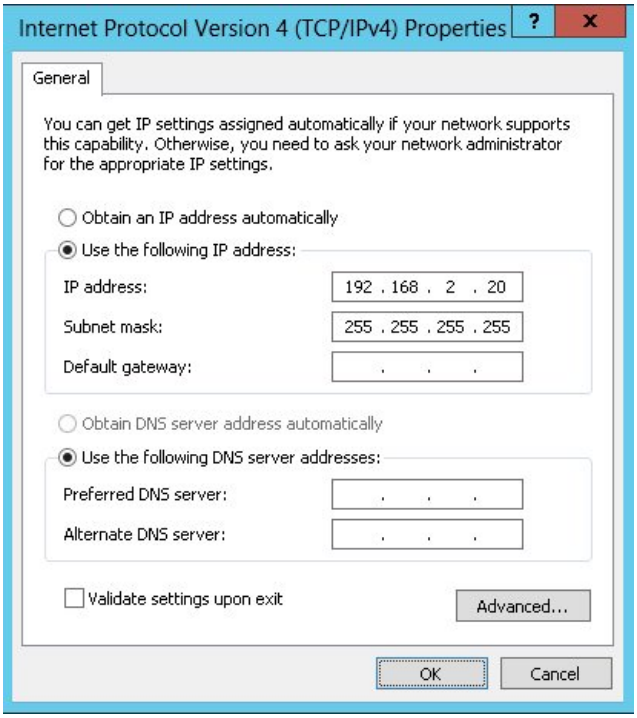
> **Important** When configuring the loopback adapter properties, make sure that **Client for Microsoft Networks** and **File & Printer Sharing for Microsoft Networks** is also checked as shown below.

IPv4 Addresses

1. Uncheck all items except **Client for Microsoft Networks**, **File & Printer Sharing for Microsoft Networks** and **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:



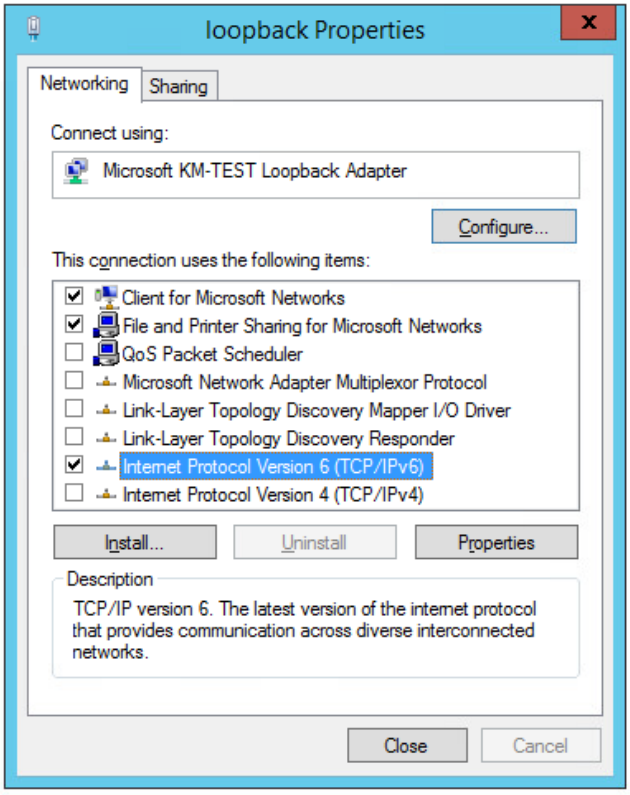
> **Note** **192.168.2.20** is an example, make sure you specify the correct VIP address.

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

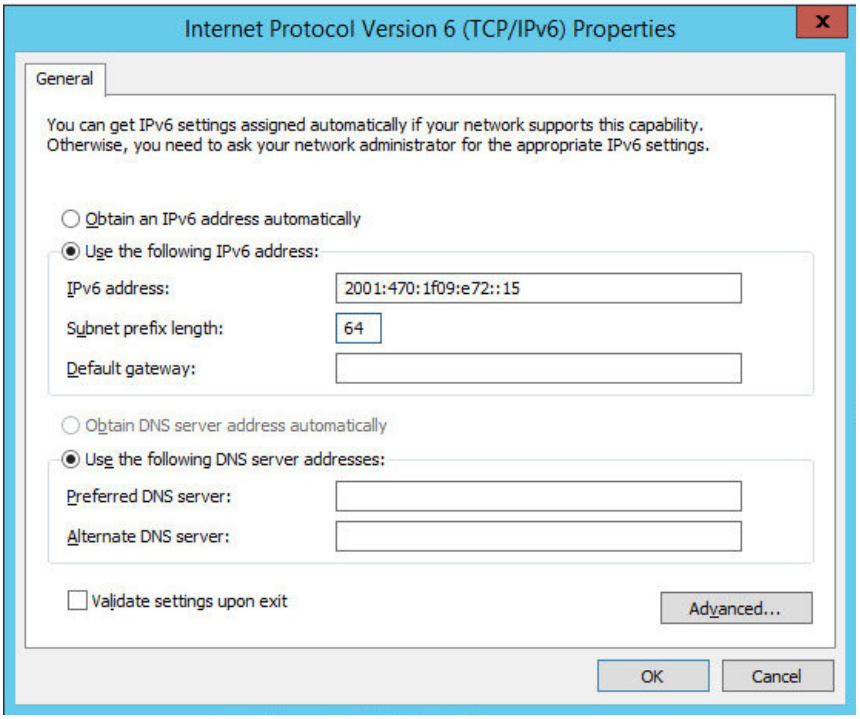
3. Click **OK** then click **Close** to save and apply the new settings.

IPv6 Addresses

1. Uncheck all items except **Client for Microsoft Networks**, **File & Printer Sharing for Microsoft Networks** and **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:

> **Important** 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
```

15.2. Configuring HA - Adding a Secondary Appliance

Our recommended configuration is to use a clustered HA pair of load balancers to provide a highly available and resilient load balancing solution. We recommend that the Primary appliance is fully configured first, then the Secondary appliance can be added to create an HA pair. Once the HA pair is configured, load balanced services must be configured and modified on the Primary appliance. The Secondary appliance will be automatically kept in sync.

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

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

Non-Replicated Settings

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

WebUI Main Menu Option	Sub Menu Option	Description
Local Configuration	Hostname & DNS	Hostname and DNS settings
Local Configuration	Network Interface Configuration	Interface IP addresses, bonding configuration and VLANs
Local Configuration	Routing	Default gateways and static routes
Local Configuration	System Date & time	Time and date related settings
Local Configuration	Physical – Advanced Configuration	Various appliance settings
Local Configuration	Portal Management	Portal management settings
Local Configuration	Security	Security settings

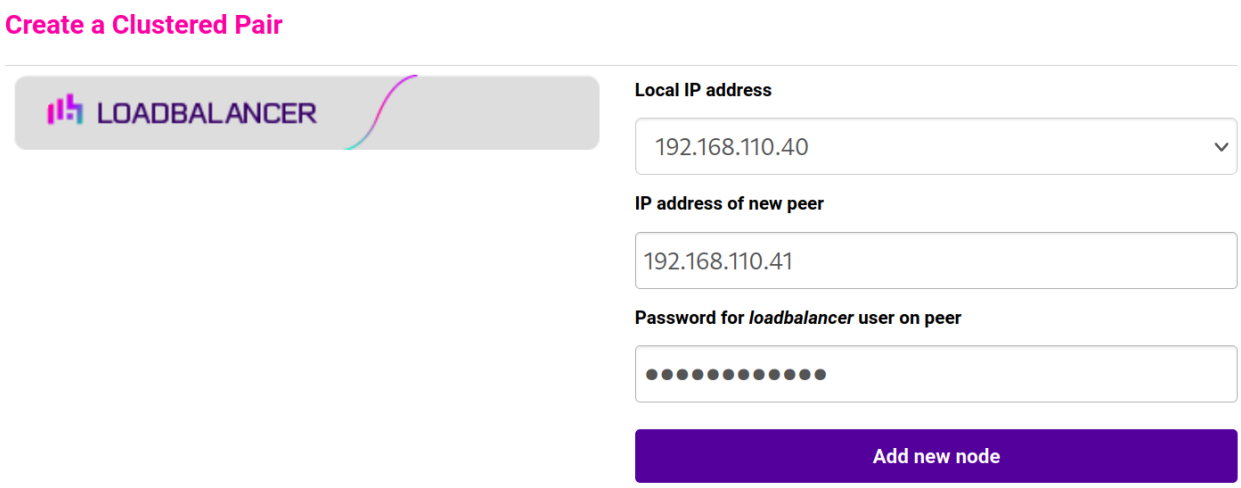
WebUI Main Menu Option	Sub Menu Option	Description
Local Configuration	SNMP Configuration	SNMP settings
Local Configuration	Graphing	Graphing settings
Local Configuration	License Key	Appliance licensing
Maintenance	Backup & Restore	Local XML backups
Maintenance	Software Updates	Appliance software updates
Maintenance	Fallback Page	Fallback page configuration
Maintenance	Firewall Script	Firewall (iptables) configuration
Maintenance	Firewall Lockdown Wizard	Appliance management lockdown settings

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

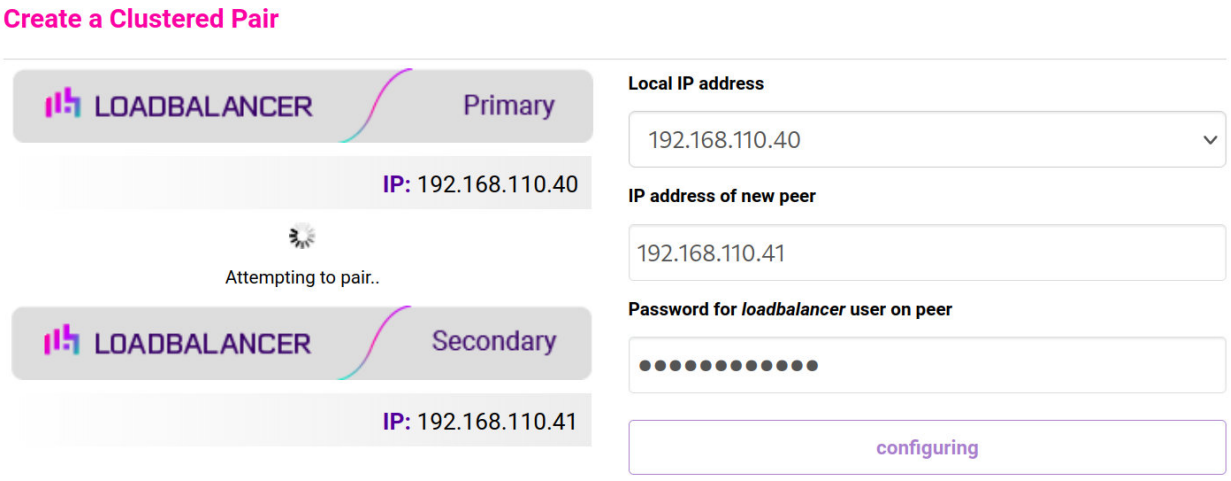
Configuring the HA Clustered Pair

> **Note** If you have already run the firewall lockdown wizard on either appliance, you'll need to ensure that it is temporarily disabled on both appliances whilst performing the pairing process.

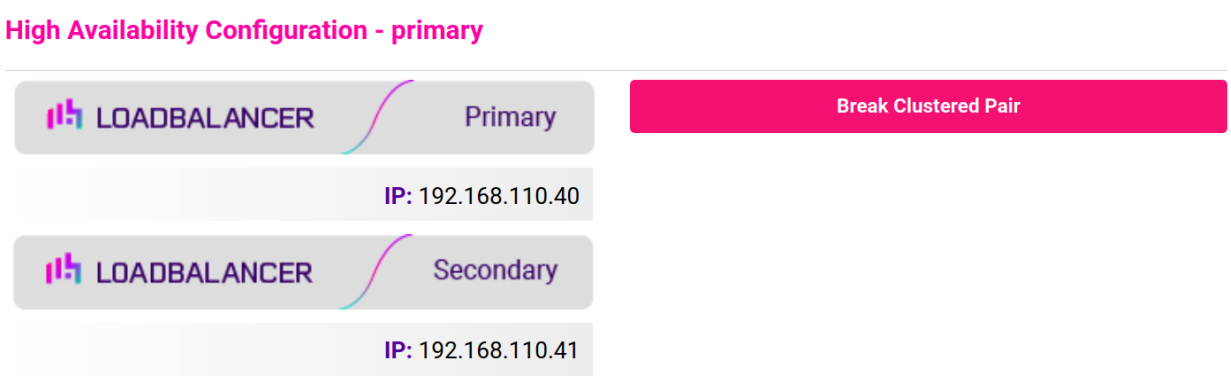
1. Deploy a second appliance that will be the Secondary and configure initial network settings.
2. Using the WebUI on the Primary appliance, navigate to: *Cluster Configuration > High-Availability Configuration*.



3. Specify the IP address and the *loadbalancer* user's password for the Secondary (peer) appliance as shown in the example above.
4. Click **Add new node**.
5. The pairing process now commences as shown below:



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



7. To finalize the configuration, restart heartbeat and any other services as prompted in the "Commit changes" message box at the top of the screen.

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

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

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

16. Document Revision History

Version	Date	Change	Reason for Change	Changed By
1.0.0	21 June 2018	Initial version		AH
1.0.1	26 June 2018	Made the guide more generic by adding additional vendor options Changed the title from 'AutoStore With Xerox EIP Connect'	Required updates	AH
1.0.2	6 December 2018	Added the new "Company Contact Information" page	Required updates	AH
1.1.0	1 August 2019	Styling and layout Changed layer 7 SNAT mode deployment method to layer 4 NAT mode Updated a Kofax hyperlink to use the new Kofax location	General styling updates Required updates	AW, AH
1.1.1	8 June 2020	New title page Updated Canadian contact details	Branding update Change to Canadian contact details	AH
1.1.2	15 October 2020	Name change from Nuance to Kofax	Kofax acquisition of Nuance Document Imaging	OW
1.2.0	1 November 2021	Converted the document to AsciiDoc	Move to new documentation system	AH, RJC, ZAC
1.2.1	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	Housekeeping across all documentation	AH
1.2.2	2 February 2023	Updated screenshots	Branding update	AH

Version	Date	Change	Reason for Change	Changed By
1.2.3	7 March 2023	Removed conclusion section	Updates across all documentation	AH
1.3.0	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.