

# Load Balancing Dispatcher Phoenix®

Version 1.2.0



# 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. Konica Minolta Dispatcher Phoenix	4
4. Konica Minolta Dispatcher Phoenix	4
5. Load Balancing Konica Minolta Dispatcher Phoenix	5
6. Load Balancer Deployment Methods	5
6.1. Layer 4 DR Mode	5
6.2. Layer 7 SNAT Mode	6
7. Dispatcher Phoenix Deployment Concept	7
8. Load Balancing Konica Minolta Dispatcher Phoenix	7
8.1. Load Balancing & HA Requirements	7
8.2. Persistence (aka Server Affinity)	8
8.3. Virtual Service (VIP) Requirements	8
8.4. Port Requirements	8
KMBS BEST Server	8
KMBS LPR Service	8
KMBS SMTP Service	8
KMBS SEC Workflow Worker Process	8
9. Loadbalancer.org Appliance – the Basics	9
9.1. Virtual Appliance	9
9.2. Initial Network Configuration	9
9.3. Accessing the Appliance WebUI	9
Main Menu Options	11
9.4. Appliance Software Update	11
Determining the Current Software Version	11
Checking for Updates using Online Update	11
Using Offline Update	12
9.5. Ports Used by the Appliance	12
9.6. HA Clustered Pair Configuration	13
10. Load Balancing Konica Minolta Dispatcher Phoenix – Using DR Mode	13
10.1. Part 1 – Prepare the Konica Minolta Servers for Load Balancing	13
Step 1 – Prerequisites	13
Step 2 – Solve the ARP Problem on Each server	13
Step 3 – Configure Registry Entries	14
Step 4 – Configure Name Resolution	14
Step 5 – Reboot Each Print Server	15
10.2. Part 2 – Configure Load Balancing for Microsoft Print Server	15
Configure the virtual service (VIP)	15
Define the Real Servers (RIPs)	16
10.3. Part 3 – Configure Load Balancing for Konica Minolta Dispatcher Phoenix	16
Configure the virtual service (VIP)	16
Define the Real Servers (RIPs)	17
11. Load Balancing Konica Minolta Dispatcher Phoenix – Using SNAT Mode	18
11.1. Part 1 – Prepare the Konica Minolta Servers for Load Balancing	18
Step 1 – Prerequisites	18
Step 2 – Configure Registry Entries	18

Step 3 – Configure Name Resolution .....	19
Step 4 – Reboot Each Print Server .....	19
11.2. Part 2 – Configure Load Balancing for Microsoft Print Server .....	20
Configure the virtual service (VIP) .....	20
Define the Real Servers (RIPs) .....	20
11.3. Part 3 – Configure Load Balancing for Konica Minolta Dispatcher Phoenix .....	21
Configure the virtual service (VIP) .....	21
Define the Real Servers (RIPs) .....	21
Finalize Settings – Reload HAProxy .....	22
12. Testing & Verification .....	22
12.1. Testing the Load Balanced Servers .....	22
12.2. Using System Overview .....	23
13. Technical Support .....	23
14. Further Documentation .....	23
15. Appendix .....	24
15.1. Solving the ARP Problem .....	24
Windows Server 2012 & Later .....	24
15.2. Configuring HA - Adding a Secondary Appliance .....	29
Non-Replicated Settings .....	29
Configuring the HA Clustered Pair .....	30
16. Document Revision History .....	32

# 1. About this Guide

This guide details the steps required to configure a load balanced Konica Minolta Dispatcher Phoenix environment utilizing Loadbalancer.org appliances. It covers the configuration of the load balancers and also any Konica Minolta Dispatcher Phoenix 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 Konica Minolta Dispatcher Phoenix. 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. Konica Minolta Dispatcher Phoenix

- All versions

## 4. Konica Minolta Dispatcher Phoenix

Konica Minolta's Dispatcher Phoenix is a powerful application that can help any business save time by automating document image processing, printing, and routing tasks via customisable workflows. With a large variety of processing features, virtually everything is possible – from cleaning up images, applying watermarks and annotations, and renaming files to routing documents to folders, FTP servers, MFPs, or e-mail recipients – and it's all fully automatic! Unique LiveFlo technology provides a real-time view of documents as they are being processed – a great way to identify bottlenecks and making sure files will reach their correct destinations. Dispatcher Phoenix provides busy offices with the convenience and flexibility they need.

The application is highly scalable up to the largest enterprise environments. Dispatcher Phoenix includes a web user interface for access to important enterprise tools – such as apps for setting up server clusters for redundancy/load balancing, failover, offloading, sharing workflows with specific users, and more. Administrators can manage their workflows (run, stop, pause) from the web as well as edit user variables and view important analytics about work being done, including the number of documents being scanned, files collected, and users



scanning.

## 5. Load Balancing Konica Minolta Dispatcher Phoenix

For Konica Minolta Dispatcher Phoenix, the preferred load balancing method is Layer 4 DR Mode (Direct Routing, aka DSR / Direct Server Return). This is a very high performance solution that requires little change to your existing infrastructure. It is necessary to solve "the ARP problem" on the real print servers. This is a straightforward process, and is detailed in [Solving the ARP Problem](#).

Where it's not feasible to use layer 4 DR mode, layer 7 SNAT mode should be used. Whilst this mode does not have the raw throughput of layer 4 methods, it still enables high performance load balancing and requires no changes to the print servers.

## 6. Load Balancer Deployment Methods

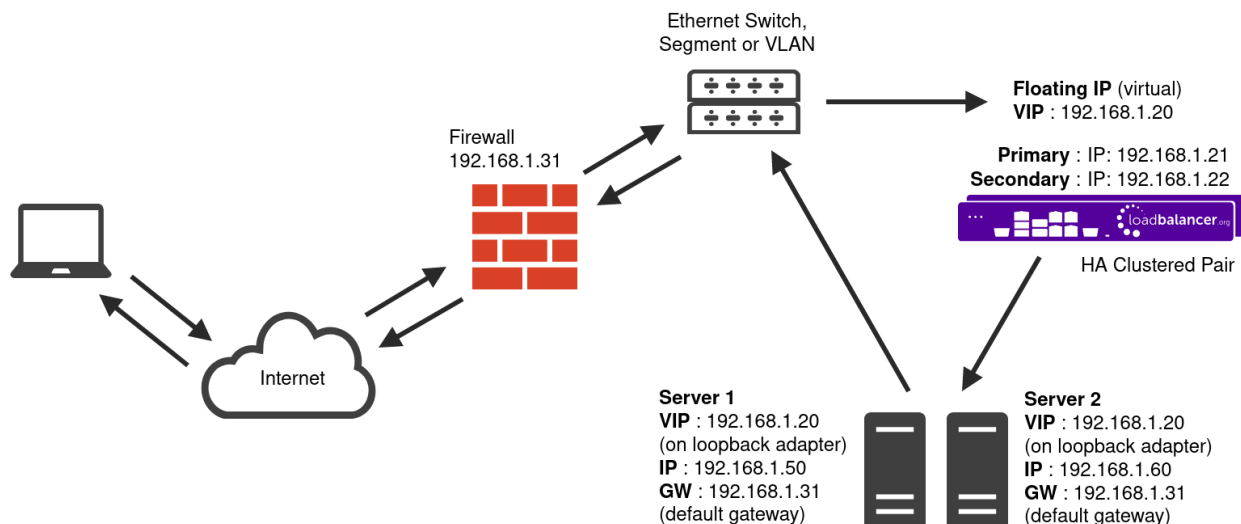
As mentioned above, Layer 4 DR mode and Layer 7 SNAT mode can be used. Both methods are described below.

### 6.1. 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*.



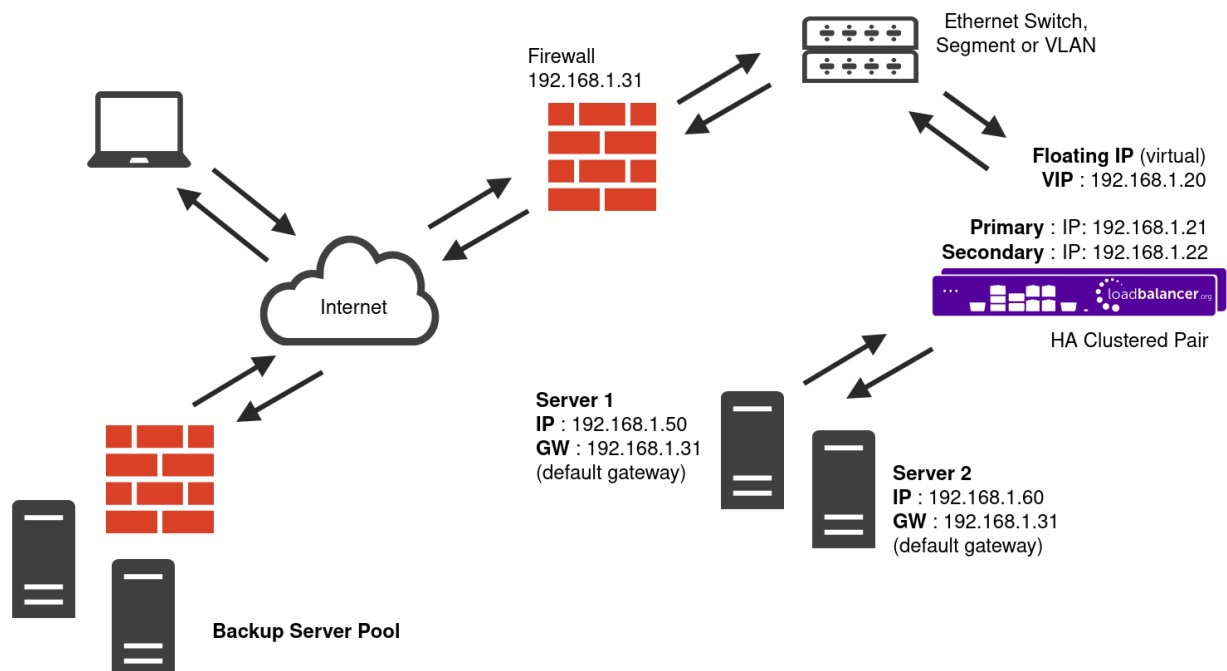
- DR mode works by changing the destination MAC address of the incoming packet to match the selected Real Server on the fly which is very fast.
- When the packet reaches the Real Server it expects the Real Server to own the Virtual Services IP address (VIP). This means that each Real Server (and the 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.

## 6.2. Layer 7 SNAT Mode

Layer 7 SNAT mode uses a proxy (HAProxy) at the application layer. Inbound requests are terminated on the load balancer and HAProxy generates a new corresponding request to the chosen Real Server. As a result, Layer 7 is typically not as fast as the Layer 4 methods. Layer 7 is typically chosen when either enhanced options such as SSL termination, cookie based persistence, URL rewriting, header insertion/deletion etc. are required, or when the network topology prohibits the use of the layer 4 methods.

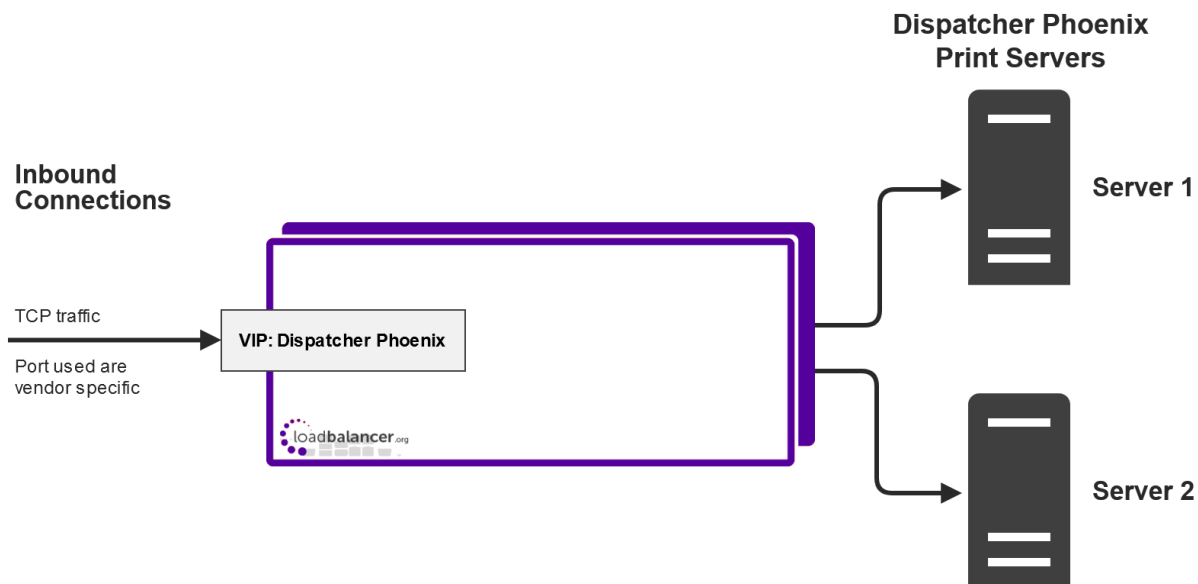


- Because layer 7 SNAT mode is a full proxy, any server in the cluster can be on any accessible subnet including across the Internet or WAN.
- Layer 7 SNAT mode is not transparent by default, i.e. the Real Servers will not see the source IP address of the client, they will see the load balancer's own IP address by default, or any other local appliance IP address if preferred (e.g. the VIP address). This can be configured per layer 7 VIP. If required, the load balancer can be configured to provide the actual client IP address to the Real Servers in 2 ways. Either by inserting a header that contains the client's source IP address, or by modifying the Source Address field of the IP packets and replacing the IP address of the load balancer with the IP address of the client. For more information on these methods please refer to [Transparency at Layer 7](#).
- Layer 7 SNAT mode can be deployed using either a one-arm or two-arm configuration. For two-arm deployments, **eth0** is normally used for the internal network and **eth1** is used for the external network

although this is not mandatory.

- Requires no mode-specific configuration changes to the load balanced Real Servers.
- Port translation is possible with Layer 7 SNAT mode, e.g. VIP:80 → RIP:8080 is supported.
- You should not use the same RIP:PORT combination for layer 7 SNAT mode VIPs and layer 4 SNAT mode VIPs because the required firewall rules conflict.

## 7. Dispatcher Phoenix Deployment Concept



VIP = **V**irtual **I**P Address

## 8. Load Balancing Konica Minolta Dispatcher Phoenix

### Note

It's highly recommended that you have a working Konica Minolta Dispatcher Phoenix environment first before implementing the load balancer.

### 8.1. Load Balancing & HA Requirements

In order to be successfully load balanced, a Konica Minolta Dispatcher Phoenix deployment must include 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 Dispatcher Phoenix deployment will already feature all of these components.

## 8.2. Persistence (aka Server Affinity)

Source IP address persistence is used for Dispatcher Phoenix servers. This ensures that a particular client will connect to the same Dispatcher Phoenix server for the duration of the session.

## 8.3. Virtual Service (VIP) Requirements

To provide load balancing and HA for Dispatcher Phoenix, 2 VIPs are used. The first VIP is for the underlying Microsoft print services and the second VIP is for the particular Konica Minolta service being load balanced.

## 8.4. Port Requirements

The following tables show the ports that are load balanced for the various Konica Minolta services:

### KMBS BEST Server

Port	Protocols	Use
50808	HTTP	KMBS BEST Server
50809	HTTPS	Secure BEST Server

### KMBS LPR Service

Port	Protocols	Use
515	TCP	LPR Service (LPD)

### KMBS SMTP Service

Port	Protocols	Use
25	TCP	Default, but configurable within SMTP Manager

### KMBS SEC Workflow Worker Process

Port	Protocols	Use
25	TCP	Output Port
53	TCP	Output Port
80	TCP	Output Port
443	TCP	Output Port
445	TCP	Output Port
465	TCP	Output Port



Port	Protocols	Use
587	TCP	Output Port

## 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:

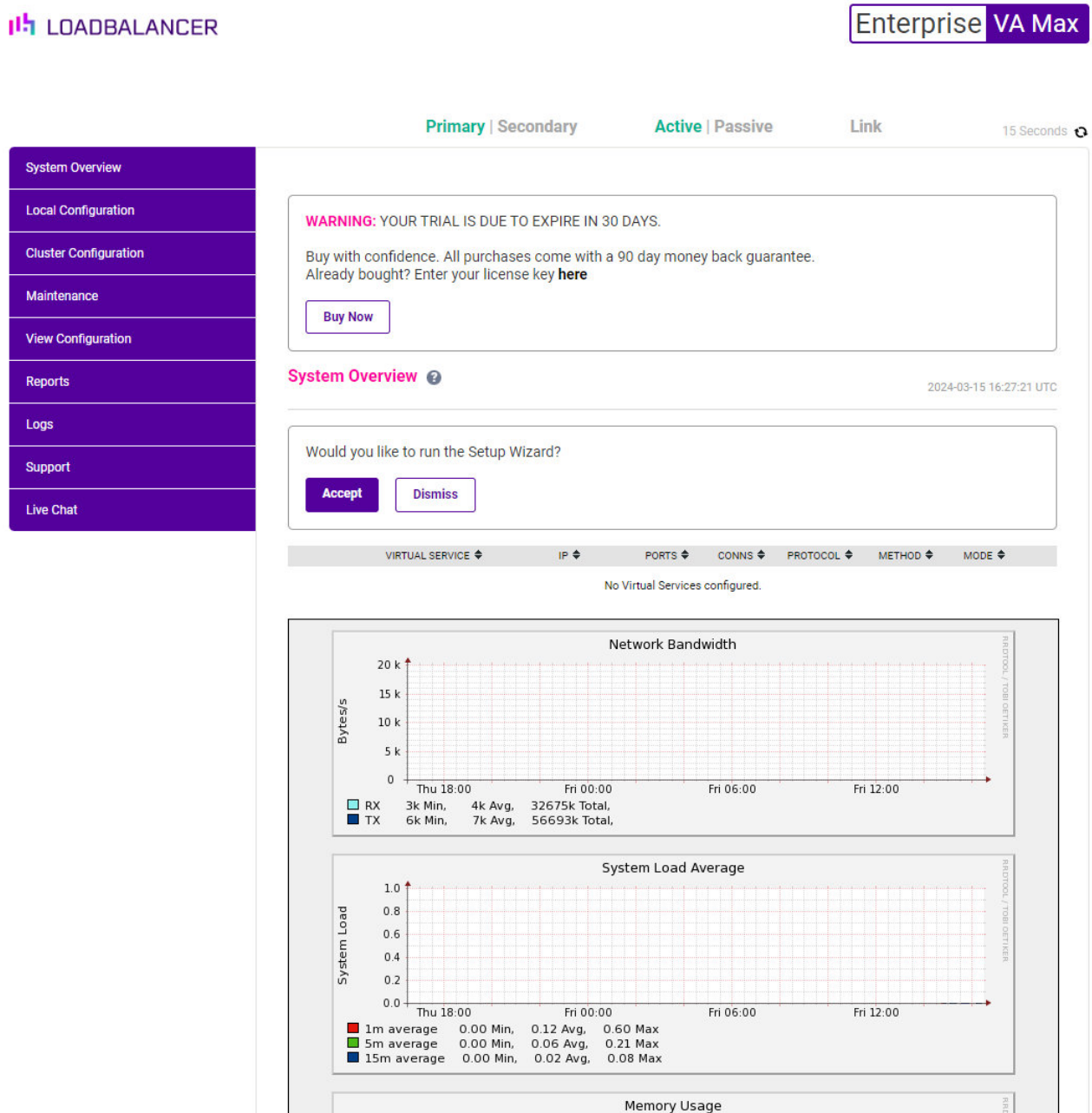
**Username:** loadbalancer

**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:

Copyright © Loadbalancer.org Inc. 2002 – 2024  
ENTERPRISE VA Max - v8.11.1

English ▼

### 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 v8.11.1 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](mailto: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:  No file chosen

Checksum:  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.

## 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
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. Load Balancing Konica Minolta Dispatcher Phoenix – Using DR Mode

## 10.1. Part 1 – Prepare the Konica Minolta Servers for Load Balancing

### Step 1 – Prerequisites

For a load balanced Konica Minolta Dispatcher Phoenix environment, each print server must comply with the following requirements:

1. Be a member of a Microsoft Windows Domain.
2. Have the **Print and Document Service** role / **Print Server** service installed.
3. Have all required printers installed and shared – the share names and permissions must be the same across all servers.
4. Have Konica Minolta Dispatcher Phoenix installed.

### Step 2 – Solve the ARP Problem on Each server



When using layer 4 DR mode, the "ARP problem" must be solved on each print 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](#).

### Step 3 – Configure Registry Entries

For the load balanced print servers, to enable them to be accessed via a shared name (**Dispatcher** is the example used in this guide), add the following registry entries to each print server:

```
Key: HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa
Value: DisableLoopbackCheck
Type: REG_DWORD
Data: 1
```

```
Key: HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\lanmanserver\parameters
Value: DisableStrictNameChecking
Type: REG_DWORD
Data: 1
```

```
Key: HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\lanmanserver\parameters
Value: OptionalNames
Type: REG_MULTI_SZ
Data: Dispatcher
```

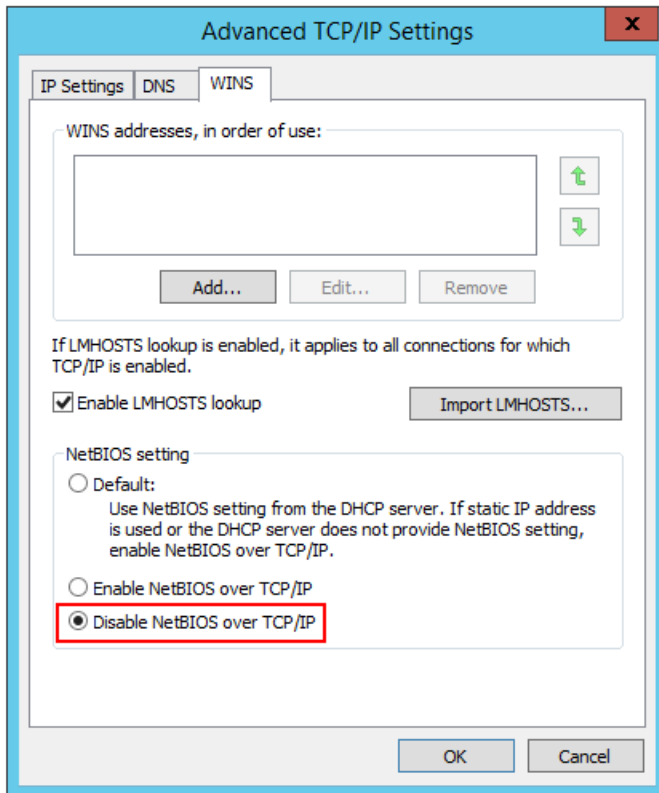
#### Note

In the example presented here, **Dispatcher** is the name that will be used to access the load balanced print servers via the virtual service (VIP) created on the load balancer. This can be set to any appropriate name. Whatever name is used, it must resolve to the IP address of the VIP.

### Step 4 – Configure Name Resolution

For printer load balancing to work, DNS name resolution should be configured. A DNS Host (A) record for the printer share name (**Dispatcher** in this example) that points at the Phoenix Dispatcher VIP (**192.168.81.10** in this example) is required.

In addition, NetBIOS over TCP/IP should be disabled on **all** interfaces on each print server as shown below:



When configuring printers to connect back to the highly available Dispatcher Phoenix, the Dispatcher Phoenix hostname / IP address should be the VIP address and not the individual Dispatcher Phoenix host name or IP address.

## Step 5 – Reboot Each Print Server

To apply all settings, reboot each print server.

## 10.2. Part 2 – Configure Load Balancing for Microsoft Print Server

### Configure the virtual service (VIP)

- Using the web user interface, navigate to *Cluster Configuration > Layer 4 – Virtual Services* and click on **Add a new Virtual Service**.

Virtual Service		
Label	<input type="text" value="PrintServers"/>	<a href="#">?</a>
IP Address	<input type="text" value="192.168.81.10"/>	<a href="#">?</a>
Ports	<input type="text" value="445"/>	<a href="#">?</a>
Protocol		
Protocol	<input type="text" value="TCP"/>	<a href="#">?</a>
Forwarding		
Forwarding Method	<input type="text" value="Direct Routing"/>	<a href="#">?</a>
		<input type="button" value="Cancel"/> <input type="button" value="Update"/>

2. Define the **Label** for the virtual service as required, e.g. **PrintServers**.
3. Set the **Virtual Service IP Address** field to the required IP address, e.g. **192.168.81.10**.
4. Set the **Ports** to **445**.
5. Leave **Protocol** set to **TCP**.
6. Leave **Forwarding Method** set to **Direct Routing**.
7. Click **Update**.

## Define 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.

Label	<input type="text" value="PS1"/>	?
Real Server IP Address	<input type="text" value="192.168.81.184"/>	?
Weight	<input type="text" value="100"/>	?
Minimum Connections	<input type="text" value="0"/>	?
Maximum Connections	<input type="text" value="0"/>	?

2. Define the **Label** for the Real Server as required, e.g. **PS1**.
3. Set the **Real Server IP Address** field to the required IP address, e.g. **192.168.81.184**.
4. Click **Update**.
5. Repeat these steps to add additional print servers as required.

## 10.3. Part 3 – Configure Load Balancing for Konica Minolta Dispatcher Phoenix

### Configure 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**.



Virtual Service		
Label	<input type="text" value="Dispatcher"/>	<a href="#">?</a>
IP Address	<input type="text" value="192.168.81.10"/>	<a href="#">?</a>
Ports	<input type="text" value="25,53,80,443,465,587"/>	<a href="#">?</a>
Protocol		
Protocol	<input type="text" value="TCP"/>	<a href="#">?</a>
Forwarding		
Forwarding Method	<input type="text" value="Direct Routing"/>	<a href="#">?</a>

2. Define the *Label* for the virtual service as required, e.g. **Dispatcher**.
3. Set the *Virtual Service IP Address* field to the required IP address, e.g. **192.168.81.10**.
4. Set the *Ports* field according to the load balanced service – please refer to [Port Requirements](#).

#### Note

If you are load balancing "KMBS SEC Workflow Worker Process", exclude port 445 from the list of ports since this port is load balanced by the Microsoft Print Server VIP configured previously.

5. Leave *Protocol* set to **TCP**.
6. Leave the *Forwarding Method* set to **Direct Routing**.
7. Click **Update**.
8. Click **Modify** next to the newly created VIP.
9. Scroll down to the *Health Checks* section and set the *Check Port* to **445**.
10. Click **Update**.

## Define 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.

Label	<input type="text" value="Phoenix1"/>	
Real Server IP Address	<input type="text" value="192.168.81.184"/>	
Weight	<input type="text" value="100"/>	
Minimum Connections	<input type="text" value="0"/>	
Maximum Connections	<input type="text" value="0"/>	

2. Define the **Label** for the Real Server as required, e.g. **Phoenix1**.
3. Set the **Real Server IP Address** field to the required IP address, e.g. **192.168.81.184**.
4. Click **Update**.
5. Repeat these steps to add additional Dispatcher Phoenix servers as required.

## 11. Load Balancing Konica Minolta Dispatcher Phoenix – Using SNAT Mode

### 11.1. Part 1 – Prepare the Konica Minolta Servers for Load Balancing

#### Step 1 – Prerequisites

For a load balanced Konica Minolta Dispatcher Phoenix environment, each print server must comply with the following requirements:

1. Be a member of a Microsoft Windows Domain.
2. Have the **Print and Document Service** role / **Print Server** service installed.
3. Have all required printers installed and shared – the share names and permissions must be the same across all servers.
4. Have Konica Minolta Dispatcher Phoenix installed.

#### Step 2 – Configure Registry Entries

For the load balanced print servers, to enable them to be accessed via a shared name (**Dispatcher** is the example used in this guide), add the following registry entries to each print server:

```
Key: HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa
Value: DisableLoopbackCheck
Type: REG_DWORD
Data: 1
```

```
Key: HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\lanmanserver\parameters
Value: DisableStrictNameChecking
```

Type: REG\_DWORD

Data: 1

Key: HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\lanmanserver\parameters

Value: OptionalNames

Type: REG\_MULTI\_SZ

Data: Dispatcher

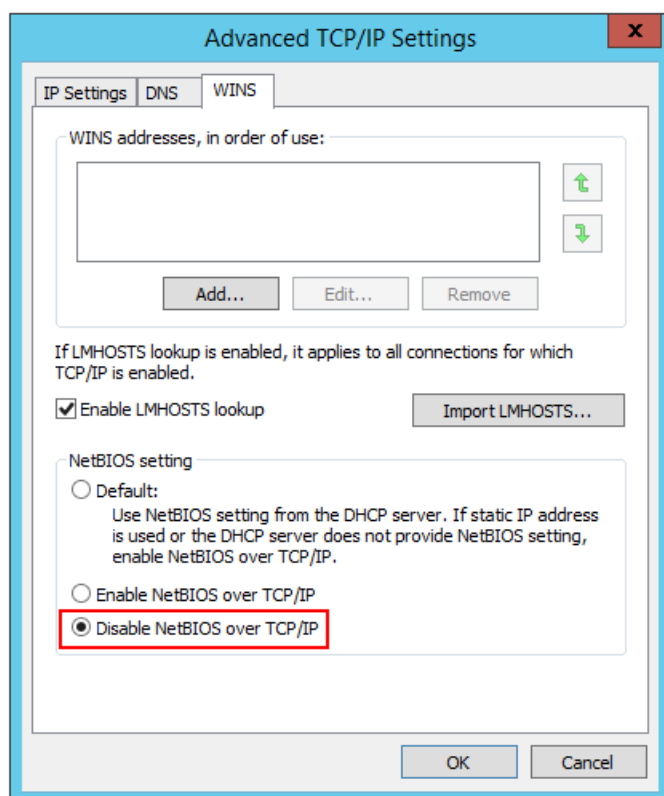
### Note

In the example presented here, **Dispatcher** is the name that will be used to access the load balanced print servers via the virtual service (VIP) created on the load balancer. This can be set to any appropriate name. Whatever name is used, it must resolve to the IP address of the VIP.

## Step 3 – Configure Name Resolution

For printer load balancing to work, DNS name resolution should be configured. A DNS Host (A) record for the printer share name (**Dispatcher** in this example) that points at the Phoenix Dispatcher VIP (**192.168.81.10** in this example) is required.

In addition, NetBIOS over TCP/IP should be disabled on **all** interfaces on each print server as shown below:



When configuring printers to connect back to the highly available Dispatcher Phoenix, the Dispatcher Phoenix hostname / IP address should be the VIP address and not the individual Dispatcher Phoenix host name or IP address.

## Step 4 – Reboot Each Print Server

To apply all settings, reboot each print server.



## 11.2. Part 2 – Configure Load Balancing for Microsoft Print Server

### Configure the virtual service (VIP)

1. Using the web user interface, navigate to *Cluster Configuration > Layer 7 – Virtual Services* and click on **Add a new Virtual Service**.

#### Layer 7 - Add a new Virtual Service

Virtual Service		[Advanced +]
Label	<input type="text" value="PrintServers"/>	?
IP Address	<input type="text" value="192.168.81.10"/>	?
Ports	<input type="text" value="445"/>	?
Protocol		
Layer 7 Protocol	<input type="text" value="TCP Mode"/>	?
		<input type="button" value="Cancel"/> <input type="button" value="Update"/>

2. Define the *Label* for the virtual service as required, e.g. **PrintServers**.
3. Set the *Virtual Service IP Address* field to the required IP address, e.g. **192.168.81.10**.
4. Set the *Ports* to **445**.
5. Set the *Layer 7 Protocol* to **TCP Mode**.
6. Click **Update**.

### Define the Real Servers (RIPs)

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

#### Layer 7 Add a new Real Server

Label	<input type="text" value="PS1"/>	?
Real Server IP Address	<input type="text" value="192.168.81.184"/>	?
Real Server Port	<input type="text"/>	?
Re-Encrypt to Backend	<input type="checkbox"/>	?
Weight	<input type="text" value="100"/>	?
		<input type="button" value="Cancel"/> <input type="button" value="Update"/>

2. Define the *Label* for the Real Server as required, e.g. **PS1**.

3. Set the *Real Server IP Address* field to the required IP address, e.g. **192.168.81.184**.
4. Leave the *Real Server Port* field blank.
5. Click **Update**.
6. Repeat these steps to add additional print servers as required.

## 11.3. Part 3 – Configure Load Balancing for Konica Minolta Dispatcher Phoenix

### Configure the virtual service (VIP)

1. Using the web user interface, navigate to *Cluster Configuration > Layer 7 – Virtual Services* and click on **Add a new Virtual Service**.

#### Layer 7 - Add a new Virtual Service

Virtual Service		[Advanced +]
Label	<input type="text" value="Dispatcher"/>	?
IP Address	<input type="text" value="192.168.81.10"/>	?
Ports	<input type="text" value="25,53,80,443,465,587"/>	?
<b>Protocol</b>		
Layer 7 Protocol	<input type="text" value="TCP Mode"/> ▼	?

Cancel Update

2. Define the *Label* for the virtual service as required, e.g. **Dispatcher**.
3. Set the *Virtual Service IP Address* field to the required IP address, e.g. **192.168.81.10**.
4. Set the Ports field according to the load balanced service – please refer to [Port Requirements](#).

#### Note

If you are load balancing "KMBS SEC Workflow Worker Process", exclude port 445 from the list of ports since this port is load balanced by the Microsoft Print Server VIP configured previously.

5. Set the *Layer 7 Protocol* to **TCP Mode**.
6. Click **Update**.
7. Click **Modify** next to the newly created VIP.
8. Scroll down to the *Health Checks* section and set the *Check Port* to **445**.
9. Click **Update**.

### Define the Real Servers (RIPs)



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

#### Layer 7 Add a new Real Server

Label	<input type="text" value="Phoenix1"/>	?
Real Server IP Address	<input type="text" value="192.168.81.184"/>	?
Real Server Port	<input type="text"/>	?
Re-Encrypt to Backend	<input type="checkbox"/>	?
Weight	<input type="text" value="100"/>	?

2. Define the *Label* for the Real Server as required, e.g. **Phoenix1**.
3. Set the *Real Server IP Address* field to the required IP address, e.g. **192.168.81.184**.
4. Leave the *Real Server Port* field blank.
5. Click **Update**.
6. Repeat these steps to add additional print servers as required.

### Finalize Settings – Reload HAProxy

To apply settings and activate the new VIPs, click the **Reload** button in the "Commit changes" box at the top of the screen.

## 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 the Load Balanced Servers

The load balanced servers can be tested either by browsing to the virtual service IP address or to the printer share name. For example:

Using the Virtual IP address (VIP):

**\\192.168.81.10**

or

Using the printer share name:

**\\Dispatcher**



Any shared printers and shared folders that have been configured on the real print servers should be visible.













## 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 Dispatcher Phoenix 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 Real Servers are healthy and available to accept connections.

### System Overview

2020-10-22 09:47:53 UTC

	VIRTUAL SERVICE ↕	IP ↕	PORTS ↕	CONNS ↕	PROTOCOL ↕	METHOD ↕	MODE ↕	
	PrintServers	192.168.81.10	445	0	TCP	Layer 4	DR	
	REAL SERVER	IP	PORTS	WEIGHT	CONNS			
	PS1	192.168.81.184	445	100	0	Drain	Halt	
	PS2	192.168.81.185	445	100	0	Drain	Halt	
	Dispatcher	192.168.81.10	53,80,443..	0	TCP	Layer 4	DR	
	REAL SERVER	IP	PORTS	WEIGHT	CONNS			
	PHOENIX1	192.168.81.184	53,80,443..	100	0	Drain	Halt	
	PHOENIX2	192.168.81.185	53,80,443..	100	0	Drain	Halt	

#### Note

This example shows layer 4 VIPs. A layer 7 configuration will look very similar.

If a particular server fails its health check, that server will be displayed red rather than green.

## 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](mailto: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

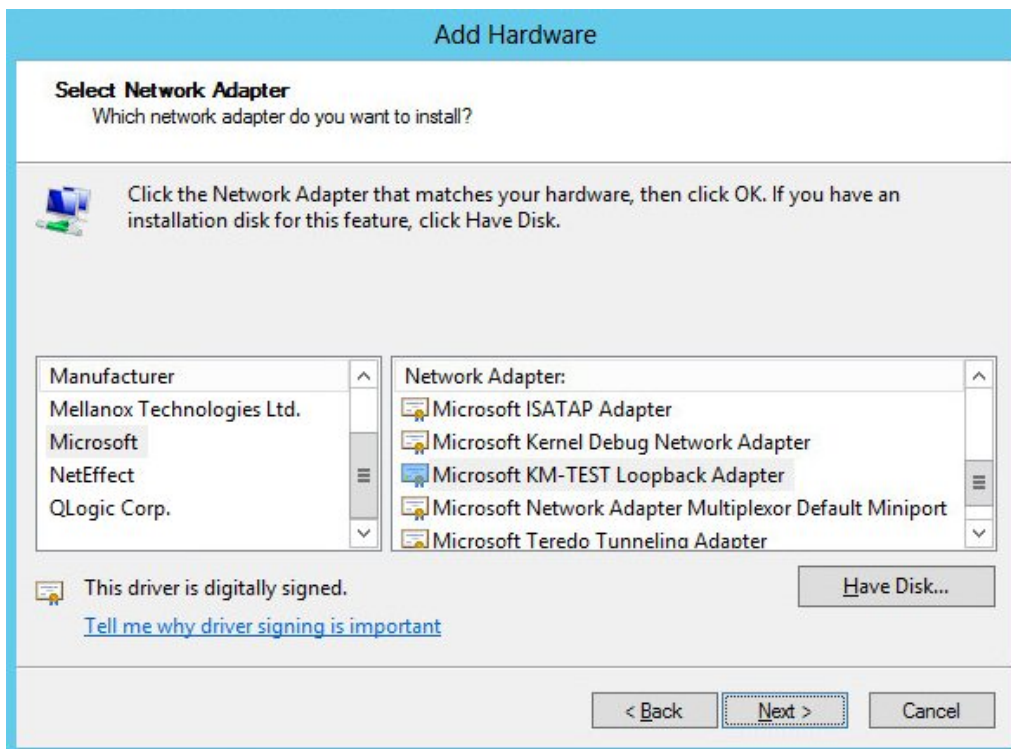
Windows Server 2012 and later support Direct Routing (DR) mode through the use of the Microsoft Loopback Adapter that must be installed and configured on each load balanced (Real) Server. The IP address configured on the Loopback Adapter must be the same as the Virtual Service (VIP) address. This enables 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

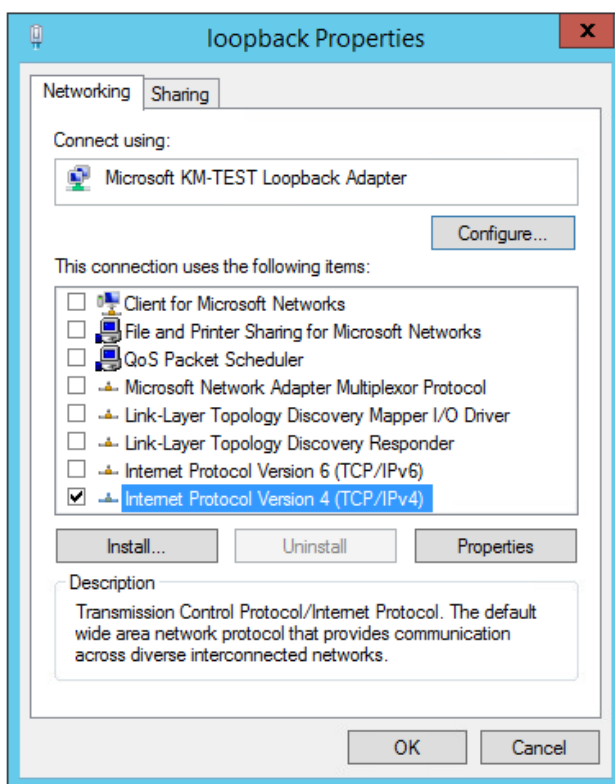
1. Open Control Panel and click **Network and Sharing Center**.
2. Click **Change adapter settings**.
3. Right-click the new Loopback Adapter and select **Properties**.

#### Note

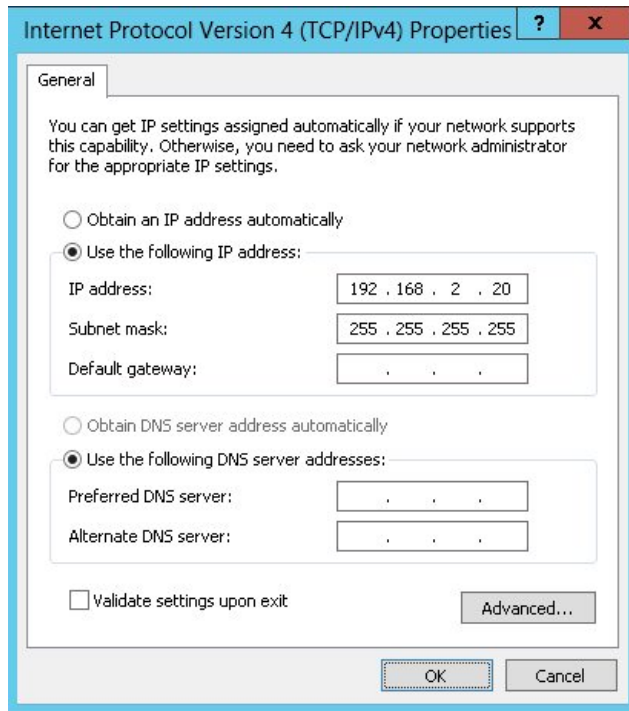
You can configure IPv4 or IPv6 addresses or both depending on your requirements.


### 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:



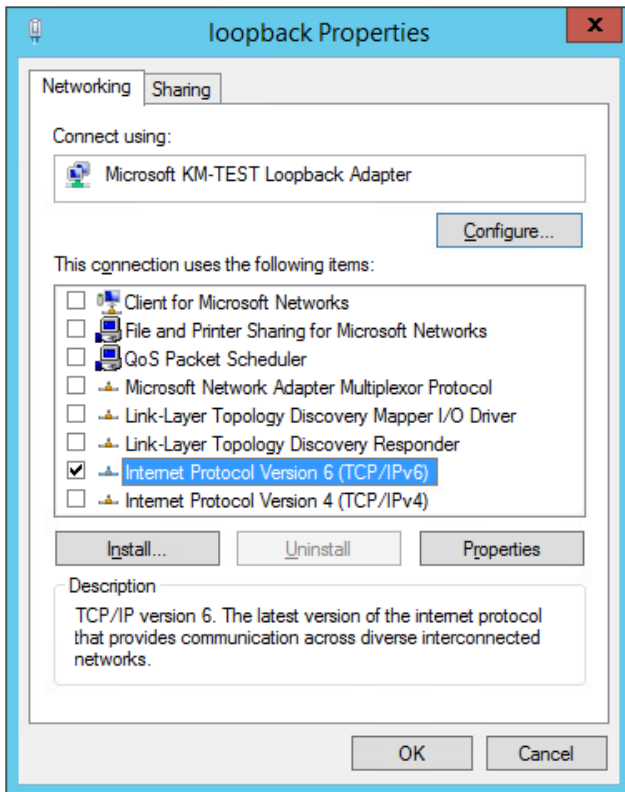
 **Note** **192.168.2.20** is an example, make sure you specify the correct VIP address.

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

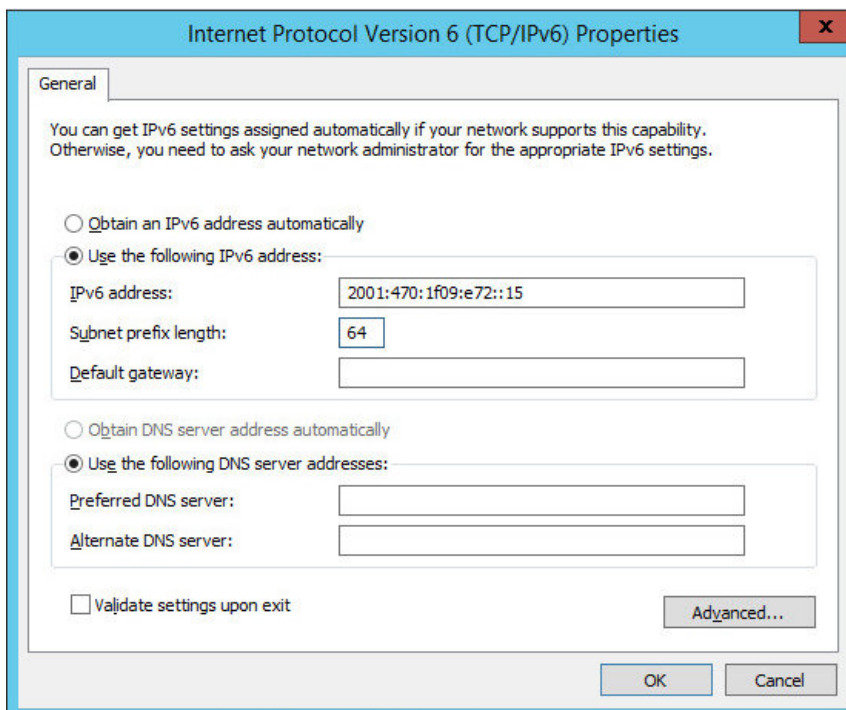
3. Click **OK** then click **Close** to save and apply the new settings.

## IPv6 Addresses

1. Uncheck all items except **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**.

### 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**

••••••••••

**Add new node**


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

 **LOADBALANCER**

Primary

IP: 192.168.110.40

  
Attempting to pair..

 **LOADBALANCER**

Secondary

IP: 192.168.110.41

Local IP address

192.168.110.40

IP address of new peer

192.168.110.41


Password for *loadbalancer* user on peer

••••••••••

configuring


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

## High Availability Configuration - primary

 **LOADBALANCER**

Primary

IP: 192.168.110.40

 **LOADBALANCER**

Secondary

IP: 192.168.110.41

Break Clustered Pair

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 October 2020	Initial version		NH, RJC
1.0.1	25 March 2021	Added section "Loadbalancer.org Appliance – the Basics"	Not included in the initial version	RJC
1.1.0	1 October 2021	Converted the document to AsciiDoc	Move to new documentation system	AH,RJC,ZAC
1.1.1	28 September 2022	Updated layer 7 VIP and RIP creation screenshots	Reflect changes in the web user interface	AH
1.1.2	5 January 2023	<p>Combined software version information into one section</p> <p>Added one level of section numbering</p> <p>Added software update instructions</p> <p>Added table of ports used by the appliance</p> <p>Reworded 'Further Documentation' section</p> <p>Removed references to the colour of certain UI elements</p>	Housekeeping across all documentation	AH
1.1.3	2 February 2023	Updated screenshots	Branding update	AH
1.1.4	7 March 2023	Removed conclusion section	Updates across all documentation	AH
1.2.0	24 March 2023	<p>New document theme</p> <p>Modified diagram colours</p>	Branding update	AH





**Visit us:** [www.loadbalancer.org](http://www.loadbalancer.org)

**Phone us:** +44 (0)330 380 1064

**Phone us:** +1 833 274 2566

**Email us:** [info@loadbalancer.org](mailto:info@loadbalancer.org)

**Follow us:** [@loadbalancer.org](https://twitter.com/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.

