# Table of Contents

1. About this Guide .............................................. 3
2. Loadbalancer.org Appliances Supported ..................... 3
3. Loadbalancer.org Software Versions Supported ............. 3
4. Kofax Equitrac Software Versions Supported ............. 3
5. Kofax Equitrac .................................................. 3
   Introduction and Overview of Different Modes ............ 3
   Prerequisites .................................................. 4
   Overview of steps required ............................... 4
7. Loadbalancer.org Appliance – the Basics ..................... 4
   Virtual Appliance ............................................. 4
   Initial Network Configuration ............................. 4
   Accessing the WebUI ......................................... 5
   Main Menu Options ......................................... 6
   HA Clustered Pair Configuration ........................... 7
8. Appliance Configuration for Kofax Equitrac – Using DR Mode ............................................... 7
   Configuring the virtual service (VIP) ..................... 7
   Defining the Real Servers (RIPS) ......................... 8
9. Appliance Configuration for Kofax Equitrac – Using SNAT Mode ............................................... 8
   Configuring the virtual service (VIP) ..................... 8
   Defining the Real Servers (RIPS) ......................... 9
10. Configuring Print Servers for Load Balancing .............. 9
    Registry Modifications ...................................... 9
    Microsoft Windows Server 2008 Specific Registry Change ............................................. 10
    Configuring Name Resolution ............................ 10
    DNS Name Resolution (Windows 2000 & later) .......... 10
    NetBIOS Name Resolution (legacy Environments) ..... 11
    Finalising the Server Configuration .................... 12
    Testing the load balanced print service ................ 12
    Installing and Configuring Couchbase and Equitrac DCE ............................................. 12
11. Technical Support ............................................. 12
12. Further Documentation ....................................... 12
13. Conclusion .................................................... 13
14. Appendix ....................................................... 14
    Solving the ARP Problem .................................. 14
    Windows Server 2012, 2016 & 2019 ...................... 14
    Configuring HA - Adding a Secondary Appliance .......... 18
15. Document Revision History .................................. 22
1. About this Guide

This guide details the steps required to configure a load balanced Kofax Equitrac environment utilizing Loadbalancer.org appliances. It covers the configuration of the load balancers and also any Kofax Equitrac 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 Equitrac. For full specifications of available models please refer to https://www.loadbalancer.org/products. Some features may not be supported in all cloud platforms due to platform specific limitations, please check with Loadbalancer.org support for further details.

3. Loadbalancer.org Software Versions Supported

- V8.4.1 and later

4. Kofax Equitrac Software Versions Supported

- Kofax Equitrac – all versions

5. Kofax Equitrac

Kofax Equitrac is a print management solution designed to simplify printer management.

Printing costs can be monitored, and can be reduced by forcing users to follow budget saving printing habits. Secure and regulations-compliant printing is made possible by allowing users to 'pick up' and print their secure documents in person at any printer. Flexible printing is achieved as users can print from anywhere, at anytime, and print from wherever they like.

6. Load Balancing Kofax Equitrac

Introduction and Overview of Different Modes

This guide details the configuration of a high availability DCE cluster for Equitrac Office and Express, using a Loadbalancer.org appliance.

For a Kofax Equitrac deployment, the preferred and default load balancer configuration uses 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 the section Configuring Print Servers for Load Balancing.

It is also possible to load balance a Kofax Equitrac deployment using Layer 7 SNAT Mode. This mode might be preferable if making changes to the real print servers is not possible, although some Windows Registry keys need to be added. Due to the increased amount of information at layer 7, performance is not as fast as at layer 4. Also note that load balanced connections at layer 7 are not source IP transparent, which is not usually an issue when load balancing print servers but should still be considered.
Prerequisites
A load balanced Kofax Equitrac environment requires the following:

- Microsoft Windows Server environment
- Installation of DCE server and Couchbase in High Availability setup

For installation instructions, refer to the Kofax support.

Overview of steps required
Setting up a load balanced Kofax Equitrac environment can be summarised as follows:

- Create a virtual service (VIP) on the load balancer that listens on the required ports
- Associate the print servers to the virtual service, i.e. define them as 'real servers' (RIPs) for the VIP
- Install and configure the Kofax Equitrac DCE Windows print servers
- Configure registry settings on the print servers to enable them to be accessed via a shared name
- Configure name resolution related settings on the print servers
- Point users at the VIP to access the print server and the printer shares

7. Loadbalancer.org Appliance – the Basics

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 The Virtual Appliance - Hypervisor Deployment and the ReadMe.txt text file included in the VA download for more detailed information on deploying the VA using various Hypervisors.

**Note**
For the VA, 4 NICs are included but only eth0 is connected by default at power up. If the other NICs are required, these should be connected using the network configuration screen within the Hypervisor.

Initial Network Configuration
After boot up, follow the instructions on the console to configure the IP address, subnet mask, default gateway, DNS and other network settings.
Important  Be sure to set a secure password for the load balancer, when prompted during the setup routine.

Accessing the WebUI
The WebUI is accessed using a web browser. Appliance authentication is based on Apache .htaccess files. User admin tasks such as adding users and changing passwords can be performed using the WebUI menu option: Maintenance > Passwords.

Note  A number of compatibility issues have been found with various versions of Internet Explorer and Edge. The WebUI has been tested and verified using both Chrome & Firefox.

Note  If required, users can also be authenticated against LDAP, LDAPS, Active Directory or Radius. For more information please refer to External Authentication.

1. Using a browser, access the WebUI using the following URL:


2. Log in to the WebUI:

   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:
The WebUI for the VA is shown, the hardware and cloud appliances are very similar. The yellow licensing related message is platform & model dependent.

3. You'll be asked if you want to run the Setup Wizard. If you click **Accept** the Layer 7 Virtual Service configuration wizard will start. If you want to configure the appliance manually, simple click **Dismiss**.

**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
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.

8. Appliance Configuration for Kofax Equitrac – Using DR Mode

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. EQDCEHA.

3. Set the Virtual Service IP Address field to the required IP address, e.g. 10.10.10.190.

4. Set the Ports as needed, depending on your MFP vendor:
   - For Lexmark and Ricoh, use port 2939.
   - For HP OXPd, use ports 2939 and 7627.

5. Click Update to create the virtual service.

6. Click Modify next to the newly created VIP.

7. Make sure that the Persistent checkbox is not selected.

8. Set the Check Port for server/service online to 2939.

9. Click Update.
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. DCE1.

3. Set the Real Server IP Address field to the required IP address, e.g. 192.168.100.20.

4. Click Update.

5. Repeat these steps to add additional print servers as required.

---


Configuring 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.

2. Define the Label for the virtual service as required, e.g. PrintService.

3. Set the Virtual Service IP Address field to the required IP address, e.g. 192.168.10.10.

4. Set the Ports to 445.

5. Set the Layer 7 Protocol to TCP Mode.

6. Click Update.
Defining 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.

2. Define the Label for the real server as required, e.g. DCE1.

3. Set the Real Server IP Address field to the required IP address, e.g. 192.168.10.20.

4. Leave the Real Server Port field blank.

5. Click Update.

6. Repeat these steps to add additional print servers as required.

7. Click on Reload HAProxy when prompted to do so in the blue box that appears. This will apply the new changes and put the new virtual service and its associated virtual servers into use.

10. Configuring Print Servers for Load Balancing

The following steps should be carried out on each print server defined in the virtual service:

1. Join the server to the same domain as the client PCs.

2. Install the Print and Document Service role / Print Server service.

3. Install and share the printers (use exactly the same share names and permissions across all servers).

4. If DR mode is used, solve the "ARP problem" on each print server, to that DR mode will work. For detailed steps on solving the ARP problem for the various versions of Windows, please refer to Solving the ARP Problem for more information.

   Important

   When configuring the Loopback Adapter to solve the ARP Problem, the following options must also be checked (ticked):

   Client for Microsoft Networks & File & Printer Sharing for Microsoft Networks

Registry Modifications

To enable the print servers to be accessed via a shared name (EQDCEHA in the example virtual service in this guide), add the following registry entries to each print server:

---

© Copyright Loadbalancer.org • Documentation • Load Balancing Kofax Equitrac 9
Microsoft Windows Server 2008 Specific Registry Change

If Microsoft Windows Server 2008 is used as the operating system for the printer servers, an additional registry entry change is required. The following registry entry should be changed from a DWORD to a QWORD:

```
Key: HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Print\DNSOneWire
Value: DnsOnWire
Type: REG_QWORD
Data: 1
```

Configuring Name Resolution

For printer load balancing to work, **either** DNS or NetBIOS name resolution should be configured as detailed below.

DNS Name Resolution (Windows 2000 & later)

To configure DNS name resolution, the following steps should be completed:

1. NetBIOS over TCP/IP should be disabled on **all** interfaces of each print server, as shown here:
2. A host name and corresponding "Host (A)" record for the virtual DCE that matches the virtual IP (VIP) address for the load balancer should be created.

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

NetBIOS Name Resolution (legacy Environments)

To configure NetBIOS name resolution, the following steps should be completed:

1. NetBIOS over TCP/IP should be **disabled on the main NIC** and **left enabled on the Loopback adapter** on each print server.

2. Either a WINS server should be set up and all clients configured to use this, or pre-loaded entries in the LMHosts file of each client should be set up.

As shown in the flow chart in [this Technet article](#), for a default H-node client, NetBIOS name resolution occurs in the following order:

1. Local NetBIOS cache.
2. WINS server.
4. Local LMHosts file.

Therefore, to avoid broadcast, LMHost entries must be declared as pre-loaded to ensure they are available in the local NetBIOS cache.
Configuring the LMHosts file
This is done by creating an entry like so:

```
EQDCEHA 192.168.100.10 #PRE
```

Entries with the #PRE directive are loaded into the cache on reboot, or can be forced using the command:

```
nbtstat -R
```

The following command can be used to view the cache and verify that the entry has been added:

```
nbtstat -c
```

**Finalising the Server Configuration**

To finalise the print server configuration changes, **each print server must be rebooted**.

**Testing the load balanced print service**

The load balanced print service can be tested, either by browsing to the virtual service IP address or the share name. In the example presented in this document, this would be done by going to

```
\10.10.10.190
```

or

```
\EQDCEHA
```

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

**Installing and Configuring Couchbase and Equitrac DCE**

The Couchbase and Equitrac DCE software should be set up by following the steps outlined in the installation document. To obtain a copy, reach out to Kofax support.

11. 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.

12. Further Documentation

13. Conclusion

Loadbalancer.org appliances provide a very cost effective solution for highly available load balanced Kofax Equitrac environments.
14. Appendix

Solving the ARP Problem

Windows Server 2012, 2016 & 2019

The basic concept is the same as for Windows 2000/2003. However, additional steps are required to set the strong/weak host behavior. This is used to either block or allow interfaces receiving packets destined for a different interface on the same server. As with Windows 2000/2003/2008, if the Real Server is included in multiple VIPs, you can add additional IP addresses to the Loopback Adapter that correspond to each VIP.

Step 1 of 3: Install the Microsoft Loopback Adapter

1. Click **Start**, then run **hdwwiz** to start the Hardware Installation Wizard.
2. When 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**.

![Add Hardware](image)

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**.
4. Uncheck all items except **Internet Protocol Version 4 (TCP/IPv4)** and **Internet Protocol Version 6 (TCP/IPv6)** as shown below:
Note

Leaving both checked ensures that both IPv4 and IPv6 are supported. Select one if preferred.

Important

When configuring the Loopback Adapter to solve the ARP Problem make sure that you also check (tick) Client for Microsoft Networks and File & Printer Sharing for Microsoft Networks as shown above.

5. If configuring IPv4 addresses select Internet Protocol Version (TCP/IPv4), click Properties and configure the IP address to be the same as the Virtual Service (VIP) with a subnet mask of 255.255.255.255, e.g. 192.168.2.20/255.255.255.255 as shown below:
6. If configuring IPv6 addresses select Internet Protocol Version (TCP/IPv6), 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:

7. Click OK on TCP/IP Properties, then click Close on Ethernet Properties to save and apply the new settings.

For Windows 2012/2016/2019, it's not necessary to modify the interface metric on the advanced tab and should be left set to Automatic.

Step 3 of 3: Configure the strong/weak host behavior
To configure the correct strong/weak host behavior for Windows 2012/2016/2019, the following commands must be run on each Real Server:

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 these commands to work, the LAN connection NIC must be named "net" and the loopback NIC must be named "loopback" as shown below. If you prefer to leave your current NIC names, then the commands above must be modified accordingly. For example, if your network adapters are named "LAN" and "LOOPBACK", the commands required would be:

```
netsh interface ipv4 set interface "LAN" weakhostreceive=enabled
netsh interface ipv4 set interface "LOOPBACK" weakhostreceive=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
```

For these commands to work, the LAN connection NIC must be named "net" and the loopback NIC must be named "loopback" as shown below. If you prefer to leave your current NIC names, then the commands above must be modified accordingly. For example, if your network adapters are named "LAN" and "LOOPBACK", the commands required would be:

```
netsh interface ipv6 set interface "LAN" weakhostreceive=enabled
netsh interface ipv6 set interface "LOOPBACK" weakhostreceive=enabled
```

Note: The names for the NICs are case sensitive, so make sure that the name used for the interface and the name used in the commands match exactly.

• Start PowerShell or use a command window to run the appropriate netsh commands as shown in the example below:
Note: This shows an IPv6 example, use the IPv4 commands if you're using IPv4 addresses.

Repeat steps 1 - 3 on all remaining Windows 2012/2016/2019 Real Server(s).

For Windows 2012/2016/2019 you can also use the following PowerShell Cmdlets:

The following example configures both IPv4 and IPv6 at the same time:

```
Set-NetIpInterface -InterfaceAlias loopback -WeakHostReceive enabled -WeakHostSend enabled -DadTransmits 0
Set-NetIpInterface -InterfaceAlias net -WeakHostReceive enabled
```

To configure just IPv4:

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

To configure just IPv6:

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

**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 should be configured first, then the Secondary should be added. Once the Primary and Secondary are paired, all load balanced services configured on the Primary are automatically replicated to the Secondary over the network using SSH/SCP.
For Enterprise Azure, the HA pair should be configured first. In Azure, when creating a VIP using an HA pair, 2 private IPs must be specified – one for the VIP when it’s active on the Primary and one for the VIP when it’s active on the Secondary. Configuring the HA pair first, enables both IPs to be specified when the VIP is created.

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

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:

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

To add a Secondary node - i.e. create a highly available clustered pair:

1. Deploy a second appliance that will be the Secondary and configure initial network settings.
2. Using the WebUI, 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 above.

4. Click Add new node.

5. The pairing process now commences as shown below:

6. Once complete, the following will be displayed:

7. 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 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](#).
<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>8 March 2018</td>
<td>Initial version</td>
<td></td>
<td>AH</td>
</tr>
<tr>
<td>1.0.1</td>
<td>6 December 2018</td>
<td>Added the new &quot;Company Contact Information&quot; page</td>
<td>Required updates</td>
<td>AH</td>
</tr>
<tr>
<td>1.1.0</td>
<td>9 December 2019</td>
<td>Styling and layout</td>
<td>General styling updates</td>
<td>AH</td>
</tr>
<tr>
<td>1.1.1</td>
<td>8 June 2020</td>
<td>New title page</td>
<td>Branding update</td>
<td>AH</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Updated Canadian contact details</td>
<td>Change to Canadian contact details</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Added standard section</td>
<td>Consistency with other deployment guides</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>'Loadbalancer.org Appliance – the Basics'</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Added standard appendix section</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>'Clustered Pair Configuration – Adding a Secondary Unit'</td>
<td></td>
<td></td>
</tr>
<tr>
<td>1.1.2</td>
<td>15th October 2020</td>
<td>Name change from Nuance to Kofax</td>
<td>Kofax Acquisition of Nuance Document Imaging</td>
<td>OW</td>
</tr>
<tr>
<td>1.2.0</td>
<td>1 November 2021</td>
<td>Converted the document to AsciiDoc</td>
<td>Move to new documentation system</td>
<td>AH, RJC, ZAC</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.