



# Load Balancing Censornet USS Gateway

Deployment Guide  
**v1.0.0**

---

## Table of Contents

1. About this Guide.....	3
2. Loadbalancer.org Appliances Supported.....	3
3. Loadbalancer.org Software Versions Supported.....	3
4. Censornet USS Gateway Versions Supported.....	3
5. Benefits of Implementing a Load Balancer.....	3
6. Load Balancer Configuration.....	4
Deployment Mode.....	4
Persistence/Server Affinity.....	4
7. Loadbalancer.org Appliance – the Basics.....	4
Virtual Appliance Download & Deployment.....	4
Initial Network Configuration.....	4
Accessing the Web User Interface (WebUI).....	5
HA Clustered Pair Configuration.....	6
8. Load Balancer & USS Gateway Configuration.....	7
Deployment Architecture.....	7
USS Gateway Configuration.....	8
Configuring the Primary Gateway.....	8
Configure Remaining Gateways.....	10
Modify the USS Gateways to accept traffic for the VIP.....	11
Load Balancer Configuration.....	12
Configure the IP Address and Hostname.....	12
Create the Virtual Service (VIP).....	12
9. Client Configuration.....	13
10. Testing & Validation.....	13
11. Technical Support.....	13
12. Further Documentation.....	14
13. Conclusion.....	14
14. Appendix.....	15
1 – Clustered Pair Configuration – Adding a Slave Unit.....	15
2 - Company Contact Information.....	17

## 1. About this Guide

This guide details the steps required to configure a load balanced Censornet USS Gateway environment utilizing Loadbalancer.org appliances. It covers the configuration of the load balancers and also any USS Gateway 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 relevant Administration Manual:

- [v7 Administration Manual](#)
- [v8 Administration Manual](#)

## 2. Loadbalancer.org Appliances Supported

The following table shows which Loadbalancer.org Appliances (hardware and virtual) can be used to load balance Censornet USS Gateway.

Discontinued Models	Current Models *
Enterprise R16	Enterprise R20
Enterprise VA R16	Enterprise MAX
Enterprise VA	Enterprise 10G
Enterprise R320	Enterprise Ultra
	Enterprise VA R20
	Enterprise VA MAX

\* For full specifications of these models please refer to: <http://www.loadbalancer.org/products/hardware>

## 3. Loadbalancer.org Software Versions Supported

- v7.6.4 and later

## 4. Censornet USS Gateway Versions Supported

- All versions

## 5. Benefits of Implementing a Load Balancer

Implementing Loadbalancer.org appliances enables multiple USS Gateways to be deployed in a cluster. This provides the following key benefits:

- **High-Availability** – If a Gateway fails, service is not interrupted

- **Maintenance** – Gateways can easily be taken out of the cluster for maintenance
- **Performance** – For additional performance simply add more Gateways to the cluster

## 6. Load Balancer Configuration

### DEPLOYMENT MODE

Layer 4 DR mode is used. In this mode, traffic from the client to the USS Gateway passes via the load balancer, return traffic passes directly back to the client which maximizes performance. Direct Routing mode works by changing the destination MAC address of the incoming packet on the fly which is very fast. This mode is transparent by default meaning that the USS Gateways see the real client IP address and not the IP address of the load balancer.

### PERSISTENCE/SERVER AFFINITY

Source IP persistence is used. When enabled (the default setting for new layer 4 VIPs), clients connecting from the same source IP address within the persistence timeout period (the default is 5 minutes) will always be sent to the same USS Gateway.

## 7. Loadbalancer.org Appliance – the Basics

### VIRTUAL APPLIANCE DOWNLOAD & DEPLOYMENT

The VA is currently available for VMware, Virtual Box, Hyper-V, KVM and XEN and has been optimized for each Hypervisor. By default, the VA is allocated 1 CPU, 2GB of RAM and has an 8GB virtual disk.

**Note:**

The Virtual Appliance can be downloaded [here](#).

**Note:**

Please refer to the [Administration Manual](#) and the ReadMe.txt text file included in the VA download for more detailed information on deploying the VA using various Hypervisors.

### INITIAL NETWORK CONFIGURATION

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

#### **Method 1 - Using the Network Setup Wizard at the console**

After boot up, follow the instructions on the console to configure the IP address, subnet mask, default gateway and DNS settings.

#### **Method 2 - Using the WebUI**

Using a browser, connect to the WebUI on the default IP address/port: **http://192.168.2.21:9080**

To set the IP address & subnet mask, use: *Local Configuration > Network Interface Configuration*

To set the default gateway, use: *Local Configuration > Routing*

To configure DNS settings, use: *Local Configuration > Hostname & DNS*

### **Method 3 - Using Linux commands**

At the console, set the initial IP address using the following command:

```
ip addr add <IP address>/<mask> dev eth0
```

At the console, set the initial default gateway using the following command:

```
route add default gw <IP address> <interface>
```

At the console, set the DNS server using the following command:

```
echo nameserver <IP address> >> /etc/resolv.conf
```

#### **Note:**

If method 3 is used, you must also configure these settings using the WebUI, otherwise the settings will be lost after a reboot.

## **ACCESSING THE WEB USER INTERFACE (WEBUI)**

The WebUI can be accessed via HTTP at the following URL: **http://192.168.2.21:9080/lbadmin**

\* *Note the port number → 9080*

The WebUI can be accessed via HTTPS at the following URL: **https://192.168.2.21:9443/lbadmin**

\* *Note the port number → 9443*

*(replace 192.168.2.21 with the IP address of your load balancer if it's been changed from the default)*

Login using the following credentials:

**Username:** loadbalancer

**Password:** loadbalancer

#### **Note:**

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

Once logged in, the WebUI will be displayed as shown on the following page:

**loadbalancer.org** Enterprise VA MAX

Master | Slave    Active | Passive    Link    5 Seconds ↻

**SYSTEM OVERVIEW** ⓘ    2015-06-18 14:21:20 UTC

Would you like to run the Setup Wizard?

Accept    Dismiss

VIRTUAL SERVICE ▾    IP ▾    PORTS ▾    CONNS ▾    PROTOCOL ▾    METHOD ▾    MODE ▾

No Virtual Services configured.

**Network Bandwidth**

Bytes/s

80 k  
60 k  
40 k  
20 k  
0

Wed 18:00    Thu 00:00    Thu 06:00    Thu 12:00

RX    2k Min,    4k Avg,    1853k Total,  
TX    11k Min,    45k Avg,    18736k Total,

**System Load Average**

System Load

1.0  
0.8  
0.6  
0.4  
0.2  
0.0

Wed 18:00    Thu 00:00    Thu 06:00    Thu 12:00

1m average    0.36 Min,    0.38 Avg,    0.39 Max  
5m average    0.09 Min,    0.13 Avg,    0.17 Max  
15m average    0.03 Min,    0.05 Avg,    0.07 Max

**Memory Usage**

Bytes

2.0 G  
1.5 G  
1.0 G  
0.5 G  
0.0

Wed 18:00    Thu 00:00    Thu 06:00    Thu 12:00

Used    117.78M Min,    122.85M Avg,    127.92M Max  
Page    79.52M Min,    79.92M Avg,    80.32M Max  
Buffer    10.86M Min,    11.14M Avg,    11.43M Max  
Free    1812.93M Min,    1819.67M Avg,    1826.41M Max

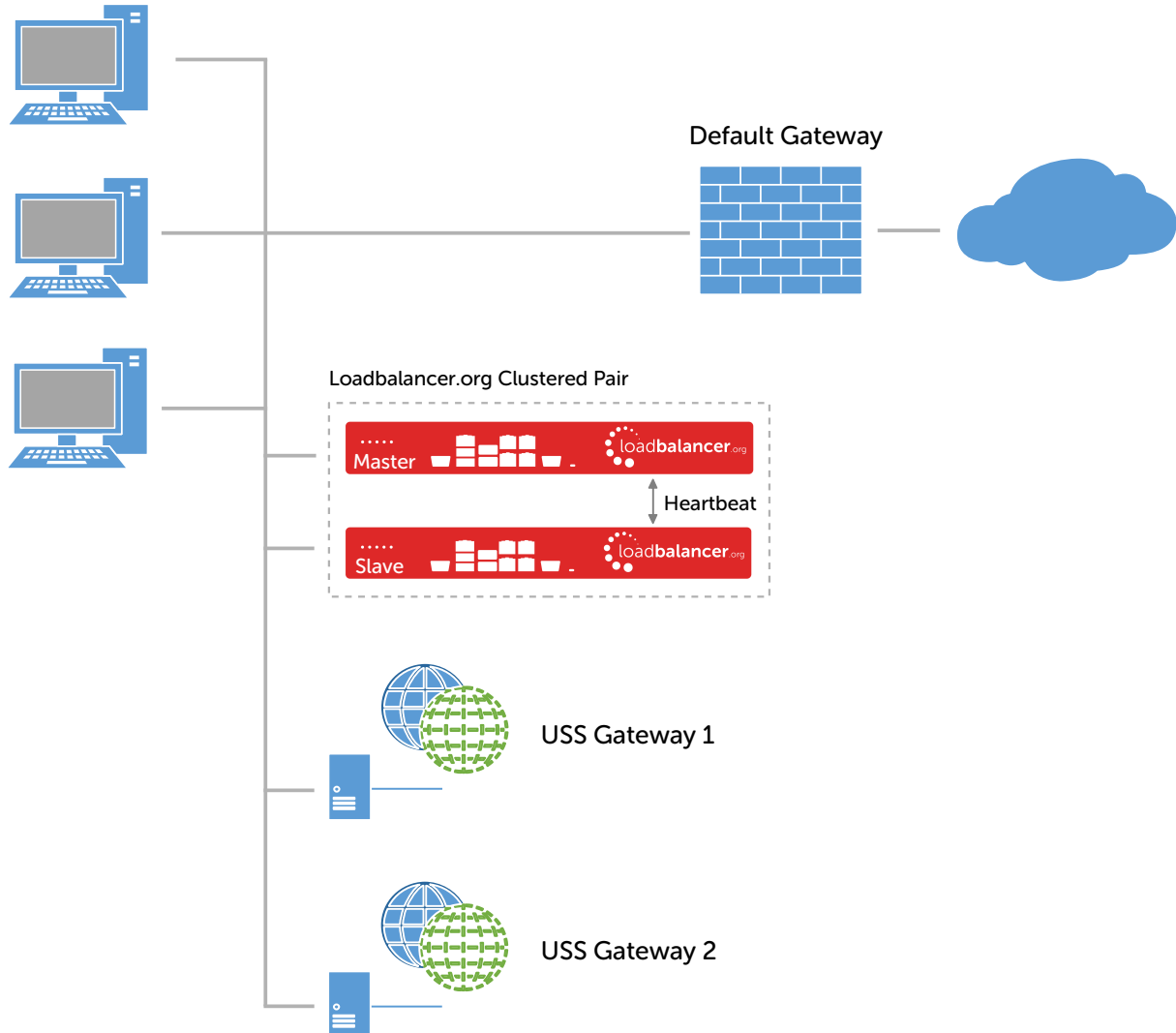
(shows v8.2.x)

## HA CLUSTERED PAIR CONFIGURATION

Loadbalancer.org recommend that load balancer appliances are deployed in pairs for high availability. In this guide a single unit is deployed first, adding a secondary slave unit is covered in section 1 of the Appendix on page [15](#).

## 8. Load Balancer & USS Gateway Configuration

### DEPLOYMENT ARCHITECTURE



#### Notes:

- Browser settings on client PC's must be changed to point at the Virtual Service (VIP) on the load balancer (see page [13](#))
- The load balancer is configured in one-arm Layer 4 DR mode
- The Censornet USS Gateways must be configured to accept traffic for the VIP (see page [11](#))
- Loadbalancer.org recommend that load balancer appliances are deployed in pairs for high availability. In this guide a single unit is deployed first, adding a secondary slave unit is covered in section 1 of the Appendix on page [15](#)
- For more information on the Censornet USS Gateway please refer to [this URL](#)

## USS GATEWAY CONFIGURATION

### CONFIGURING THE PRIMARY GATEWAY

1. Choose one of the Gateways to act as the primary gateway for the purposes of configuration
2. Decide on the hostname and IP address that you want the load balanced proxy service to use, e.g. **filter** and **10.0.0.1**
3. Using the *Network Interfaces* and *Settings* sections in the WebUI temporarily configure the primary Gateway to have that hostname and IP address as shown in the example below:

Interface	Name	IP address	Portal	Status	Running
eth0		10.0.0.125	On	Up	Yes
eth1		10.0.0.154		Down	No

Configuration

Interface: eth0

Friendly name:

IP address (IPv4): 10.0.0.1

Netmask: 255.255.255.0

Network Settings

Default Gateway: 10.0.0.254

Primary DNS: 10.0.0.2

Secondary DNS: 8.8.8.8

Hostname: filter

This will form part of the FQDN that will eventually be used by end user devices to reference the proxy

4. Reboot the Gateway to ensure the new changes have fully taken effect
5. Now join the Gateway to your Active Directory domain. This can be done by following [these instructions](#) to add a domain, join the domain and finally create the DNS entry. In this example, the DNS entry **filter.uss.local** must correctly resolve to **10.0.0.1**. The result should be a successfully joined domain configuration entry as shown in the example below:

Realms	Domain	Pre-Win 2000 Domain	Hostname	IP Address	Default	Joined	Keys
USS.LOCAL	uss.local	AD2012	dc	10.0.0.1	Yes	Yes	Yes



The important parts to check here are:

1. Joined is in **green** and says **YES**
  2. Keys is in **green** and says **YES**
6. Test that the gateway is working as expected by [configuring a domain computer](#) with the proxy **filter.uss.local** and port **8080**. You will also need to install the [SSL Certificate](#) from the gateway. This can be done by pointing the browser at **http://filter.uss.local/ussgw.der** and installing the certificate in the browsers *Trusted Root Authority* section

**Note:**

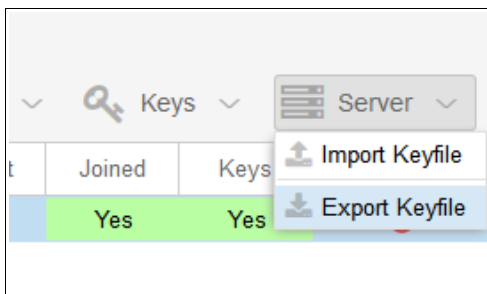
If you're unable to browse, ensure that the DNS entry for the FQDN has been set up and correctly propagated on the network.

**Note:**

Also ensure that the date/time on the Gateway is within 5 minutes of the time on the Active Directory domain controller that the Gateway has joined. This is important for the Kerberos protocol.

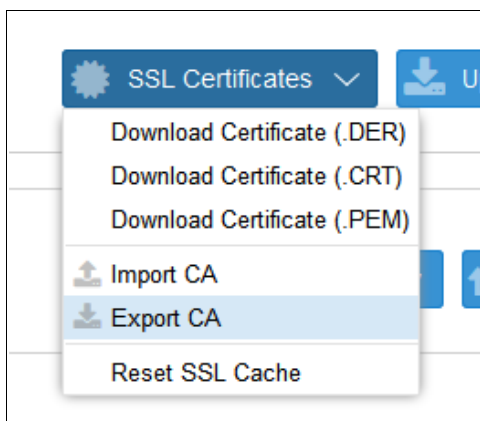
Assuming this works as expected, the next step is to export the Kerberos Keyfile and SSL certificate from this Gateway to use on the other Gateways that will be part of the load balanced cluster

7. To export the Keytab file, navigate to the *Configure > Authentication* section, select the *Server* menu and click **Export Keyfile**



Ensure that you save the Keyfile somewhere safe on your PC

8. To export the SSL certificate, go to the *System* section, click the *SSL Certificates* menu and click **Export CA**



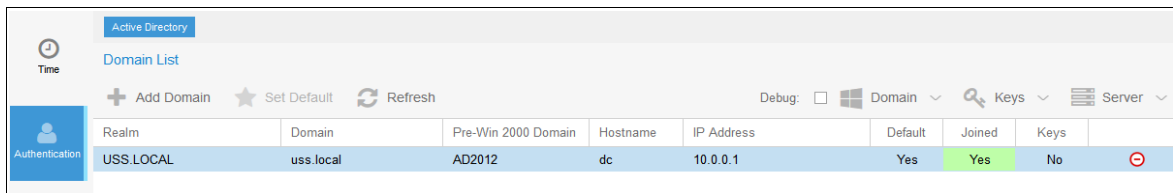
Ensure that you save the CA file somewhere safe on your PC

- Finally, repeat the first steps from this section to reconfigure this Gateway with a unique hostname and IP that it will use as part of the cluster. For example, set its hostname to **gateway1** and its IP address to **10.0.0.5**. This frees up the **filter** hostname and **10.0.0.1** IP address for the load balancer's Virtual Service to use

## CONFIGURE REMAINING GATEWAYS

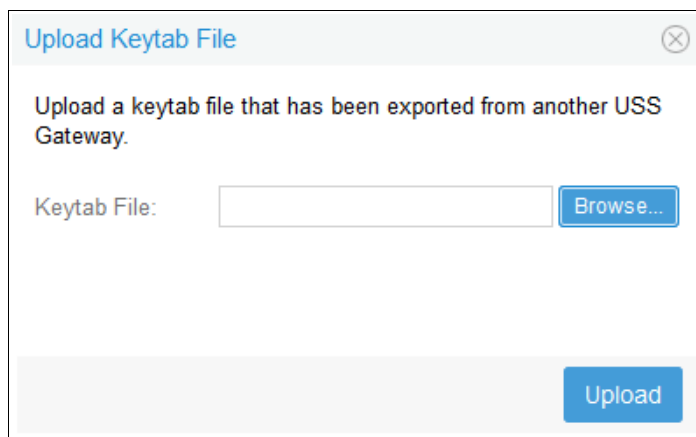
On the remaining gateways complete the following steps:

- Navigate to the *Network Interfaces* section and *Settings* section to set the desired hostname and IP address
- Next, navigate to the *Configure > Authentication* section and add the same domain as you did in the primary Gateway configuration. Also join the domain but do not create the keys

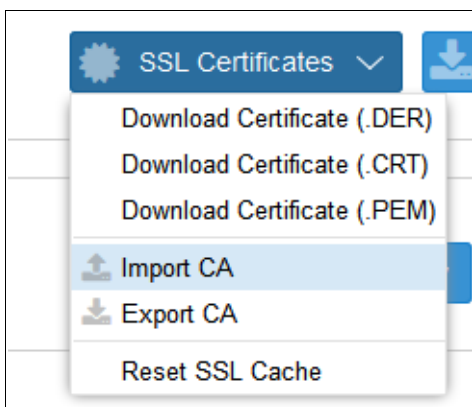


Realm	Domain	Pre-Win 2000 Domain	Hostname	IP Address	Default	Joined	Keys	Server
USS.LOCAL	uss.local	AD2012	dc	10.0.0.1	Yes	Yes	No	⊘

- Click the *Server* option and then the *Import Keytab* option



- Click **Browse** and navigate to the Keytab file that was downloaded as part of the section *Configuring the Primary Gateway* on page [8](#)
- Click **Upload**.
- Navigate to the *System* section, click the *SSL Certificates* menu and then click **Import CA**



Upload CA File
✕

The certificate file must be in PEM format and include both the certificate and private key in the same file.

This may take 10-20 seconds and will restart the proxy service.

CA File (.pem):  Browse...

Upload

Click **Browse** and navigate to the CA file that was downloaded as part of the section *Configuring the Primary Gateway* on page [8](#)

## MODIFY THE USS GATEWAYS TO ACCEPT TRAFFIC FOR THE VIP

### Note:


This final step must be followed on all Gateways.


### Concept


To enable DR mode to function, changes are required to the real servers, i.e. the USS Gateways. The real servers must accept traffic for the VIP, but they must not respond to any ARP requests for that IP, only the VIP should do this.


### Configuring the Censornet USS Gateway Appliances


1. Using the USS Gateway's WebUI, navigate to: *Configure > Advanced*
2. Enter the IP address of the VIP created on the load balancer, .e.g. **10.0.0.1**

  
Overview


  
Configure


  
Deploy

  
Network

  
System

#### Advanced Settings

  
Time

  
Authentication

Reduce noise from background Web requests to increase performance and report visibility

Reuse the same key when using temporary/ephemeral Diffie-Hellman key exchanges

Loadbalancer VIP:

3. Click the **Save** button

## LOAD BALANCER CONFIGURATION

### CONFIGURE THE IP ADDRESS AND HOSTNAME

- Using one of the methods described on page [4](#), configure an appropriate IP address for the appliance's eth0 network interface, e.g. **10.0.0.2/24**

**Note:**

Based on the example values used in this guide, do not use **10.0.0.1** – this is reserved for the Virtual Service (VIP). This IP was used when configuring the Primary Gateway as described on page [8](#).

- Using the WebUI, navigate to: *Local Configuration > Hostname & DNS*
- Set the hostname to an appropriate value, e.g. **filter**

**Note:**

The hostname '**filter**' was used when configuring the Primary Gateway as described on page [8](#).

- Click **Update**

### CREATE THE VIRTUAL SERVICE (VIP)

- Using the WebUI, navigate to: *Cluster Configuration > Layer 4 – Virtual Services*
- Click **Add a New Virtual Service**
- Enter the following details:

Label	<input type="text" value="Proxy-VIP"/>	<a href="#">?</a>
Virtual Service	IP Address <input type="text" value="10.0.0.1"/>	<a href="#">?</a>
	Ports <input type="text" value="8080"/>	<a href="#">?</a>
Protocol	<input type="text" value="TCP"/>	<a href="#">?</a>
Forwarding Method	<input type="text" value="Direct Routing"/>	<a href="#">?</a>
		<input type="button" value="Cancel"/> <input type="button" value="Update"/>

- Enter an appropriate label (name) for the VIP, e.g. **Proxy-VIP**
- Set the *Virtual Service IP address* field to the required IP address, e.g. **10.0.0.1**
- Set the *Virtual Service Ports* field to the required port, e.g. **8080**
- Ensure that *Protocol* is set to **TCP**
- Ensure that *Forwarding Method* is set to **Direct Routing**
- Click **Update**

### Define the Real Servers (RIPs)

- Using the WebUI, navigate to: *Cluster Configuration > Layer 4 – Real Servers*

2. Click **Add a new Real Server** next to the newly created VIP
3. Enter the following details:

Label	<input type="text" value="USS-Gateway1"/>	?
Real Server IP Address	<input type="text" value="10.0.0.5"/>	?
Weight	<input type="text" value="100"/>	?
Minimum Connections	<input type="text" value="0"/>	?
Maximum Connections	<input type="text" value="0"/>	?

4. Enter an appropriate label (name) for the first USS Gateway, e.g. **USS-Gateway1**
5. Change the *Real Server IP Address* field to the required IP address, e.g. **10.0.0.5**
6. Click **Update**
7. Repeat the above steps to add your other USS Gateway(s)

## 9. Client Configuration

Client Web browser settings must be configured to connect via the VIP on the load balancer. In a Microsoft based LAN environment, this is typically achieved using AD Group Policy. Please refer to [this.. Censornet URL](#) for details on configuring client Web browsers.

## 10. Testing & Validation

To verify that traffic is passing correctly through the load balancer, the following WebUI reporting options can be used on the load balancer:

*System Overview*

*Reports > Layer 4 Status*

*Reports > Layer 4 Current Connections*

Various reporting options are also available in the Censornet USS Gateway user interface. For more details please refer to the appropriate Censornet documentation.

## 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](mailto:support@loadbalancer.org)

## 12. Further Documentation

The Administration Manual contains much more information about configuring and deploying the appliance. It's available here: <http://pdfs.loadbalancer.org/loadbalanceradministrationv8.pdf>

## 13. Conclusion

Loadbalancer.org appliances provide a very cost effective solution for highly available load balanced Censornet USS Gateway environments.

## 14. Appendix

### 1 – CLUSTERED PAIR CONFIGURATION – ADDING A SLAVE UNIT

If you initially configured just the master unit and now need to add a slave - our recommended procedure, please refer to the relevant section below for more details:

**Note:**

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

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

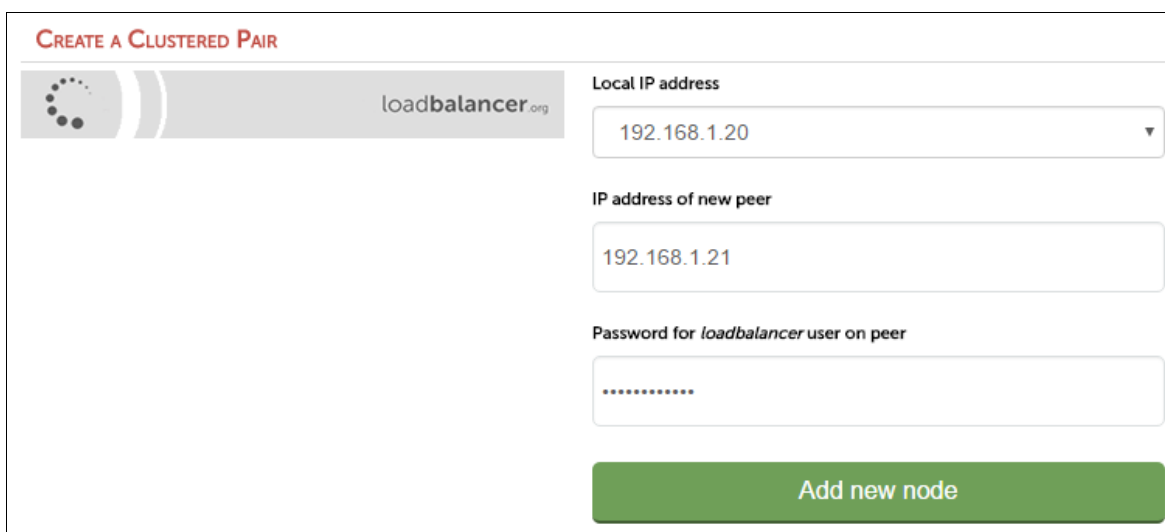
**Version 7:**

Please refer to **Chapter 8 – Appliance Clustering for HA** in the [v7 Administration Manual](#).

**Version 8:**

*To add a slave node – i.e. create a highly available clustered pair:*

- Deploy a second appliance that will be the slave and configure initial network settings
- Using the WebUI, navigate to: *Cluster Configuration > High-Availability Configuration*



**CREATE A CLUSTERED PAIR**

loadbalancer.org

Local IP address  
192.168.1.20

IP address of new peer  
192.168.1.21

Password for loadbalancer user on peer  
.....

Add new node

- Specify the IP address and the *loadbalancer* users password (the default is 'loadbalancer') for the slave (peer) appliance as shown above
- Click **Add new node**
- The pairing process now commences as shown below:

**CREATE A CLUSTERED PAIR**

	192.168.1.20	loadbalancer.org	Local IP address	192.168.1.20
Attempting to pair..			IP address of new peer	192.168.1.21
	192.168.1.21	loadbalancer.org	Password for <i>loadbalancer</i> user on peer	.....
				configuring

- Once complete, the following will be displayed:

**HIGH AVAILABILITY CONFIGURATION - MASTER**

	192.168.1.20	loadbalancer.org	<b>Break Clustered Pair</b>
	192.168.1.21	loadbalancer.org	

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

**Note:**

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

**Note:**

Please refer to chapter 9 – Appliance Clustering for HA in the [Administration Manual](#) for more detailed information on configuring HA with 2 appliances.



## 2 - COMPANY CONTACT INFORMATION

<b>Website</b>	URL: <a href="http://www.loadbalancer.org">www.loadbalancer.org</a>
<b>North America (US)</b>	<p>Loadbalancer.org, Inc.  4250 Lancaster Pike, Suite 120  Wilmington  DE 19805  USA</p> <p>Tel: +1 888.867.9504  Fax: +1 302.213.0122  Email (sales): <a href="mailto:sales@loadbalancer.org">sales@loadbalancer.org</a>  Email (support): <a href="mailto:support@loadbalancer.org">support@loadbalancer.org</a></p>
<b>North America (Canada)</b>	<p>Loadbalancer.org Ltd  300-422 Richards Street  Vancouver, BC  V6B 2Z4  Canada</p> <p>Tel: +1 866.998.0508  Fax: +1 302.213.0122  Email (sales): <a href="mailto:sales@loadbalancer.org">sales@loadbalancer.org</a>  Email (support): <a href="mailto:support@loadbalancer.org">support@loadbalancer.org</a></p>
<b>Europe (UK)</b>	<p>Loadbalancer.org Ltd.  Compass House  North Harbour Business Park  Portsmouth, PO6 4PS  UK</p> <p>Tel: +44 (0)330 3801064  Fax: +44 (0)870 4327672  Email (sales): <a href="mailto:sales@loadbalancer.org">sales@loadbalancer.org</a>  Email (support): <a href="mailto:support@loadbalancer.org">support@loadbalancer.org</a></p>
<b>Europe (Germany)</b>	<p>Loadbalancer.org GmbH  Tengstraße 27  D-80798  München  Germany</p> <p>Tel: +49 (0)89 2000 2179  Fax: +49 (0)30 920 383 6495  Email (sales): <a href="mailto:vertrieb@loadbalancer.org">vertrieb@loadbalancer.org</a>  Email (support): <a href="mailto:support@loadbalancer.org">support@loadbalancer.org</a></p>