

What's in the box?

- LoadMaster *Exchange* appliance
- Power cable
- Serial cable
- Document CD
- Mounting brackets

This guide is designed to get your LoadMaster *Exchange* on to your network quickly, so that you can administer it from your browser and be up and running in the shortest time.

Before you continue with this guide, you must have preconfigured your Exchange 2010 environment to allow for SSL offloading.

Your license (or licensing guide) has been provided on the sheet in the box.

1 – Installation

To install the LoadMaster:

1. Install into 19" rack or other safe location.
2. Connect Ethernet cables to the ports on the LoadMaster *Exchange*. Please use the worksheet included to determine which ports you will need to connect. (For single arm setups, you will only need to connect your switch to port 0).
3. Connect the power cable to the LoadMaster *Exchange*.
4. Turn on power to the unit.

2 – Connect to the Web User Interface (WUI)

Using a PC that is connected to the same network as the LoadMaster *Exchange*, or a PC that can reach that network:

1. Open an https browser window to the **default IP address: https://192.168.1.101**.
2. Login with:
 - a. Login: **bal**
 - b. Password: **1fourall**
3. If you did not yet license the LoadMaster *Exchange*, you will be prompted to enter it here. This may have been provided to you in the box. Contact KEMP Technologies if you did not receive a license. Note: The Access Code on screen may not match the one on your license. This is unusual and will not be an issue with the license..
4. You will be prompted to change the password, do this and reauthenticate using your new credentials.
5. The WUI should reflect your license and be fully configurable. If you do not see any menu options, refresh your browser.

3 – Network IP Configuration

Next you need to assign valid IP addresses to your LoadMaster *Exchange* such that it can be seen on the network. You will need to define IP addresses for:

- Network side of the LoadMaster *Exchange*
- Server side of the LoadMaster *Exchange* if two armed.

- Four (4) preconfigured Virtual Service
- *Real Servers (CAS array) in your configuration*
- Default Gateway

From your browser, that should still be connected to the LoadMaster *Exchange*, on the left side of the screen click:

1. **System Configuration > Interfaces > eth0** to input the Network address. If two armed, repeat this step for eth1.
2. **System Configuration > Route Management > Default Gateway** to input the Default gateway address.
3. **Virtual Services > View/Modify Services > Modify** of Virtual Service 1. Click **Change Address** and input the IP address for this virtual service.
4. Scroll down the screen to the section **Real Servers** for this Virtual Service. Click **Add New** and input the Real Server (CAS) IP address and do not change any other parameter on that screen. Click **Add this Real Server** to finish.
5. **System Configuration > Sys Admin > System Reboot** and click the **Reboot** button.

Repeat steps 3 and 4 for each preconfigured Virtual Service.

If you are running a single LoadMaster *Exchange*, no further configuration is necessary and your appliance should be operational for the preconfigured services.

4 – High Availability

If you are configuring a pair of LoadMaster *Exchange* units in a high availability mode, you must ensure the first appliance (HA1) is properly configured before the second one (HA2) is powered on. Setting up the second appliance is similar to setting up the first. HA2 Setup is as follows:

Follow steps 1 to 5 in section 2, Connect to the Web user Interface, of this guide.

6. You will be asked to assign the network side IP Address.
7. You will then be asked to enter the IP address you gave the network side of the HA1 unit.
8. The HA2 unit will automatically pull the configuration data from the HA1 unit.
9. Reboot the HA2 unit.

If you are using a one armed Configuration, then it is beneficial to connect the Eth1 ports of the LoadMasters directly together via a patch cable. No further configuration is necessary.

5 - Bonding and VLANs

If you are planning on bonding interfaces or setting up VLAN trunking, please refer to the Bonding and VLAN sections of the LoadMaster 5.1 Installation and Configuration Guide, located at <http://www.kemptechnologies.com/documentation>.

Turn over for MS Exchange services configurations

Main Menu (bal)

- Home
- Virtual Services
- Statistics
- Real Servers
- Rules & Checking
- Certificates
- System Configuration

Virtual Services

	Virtual IP Address	Prot	Name	Layer	Certificate Installed	Scheduler	Status	Real Servers
1	192.168.1.254.*	tcp	RPC Client Access Service	L7		round robin	Down	<input type="button" value="Modify"/> <input type="button" value="Delete"/>
2	192.168.1.254:25	tcp	Hub-Edge-SMTP	L7		least connection	Down	<input type="button" value="Modify"/> <input type="button" value="Delete"/>
3	192.168.1.254:80	tcp	Enforce Secure Access	L7		round robin	Redirect	<input type="button" value="Modify"/> <input type="button" value="Delete"/>
4	192.168.1.254:443	tcp	All HTTPS Services -OWA OA EAS	L7	<input type="button" value="Add New"/>	round robin	Down	<input type="button" value="Modify"/> <input type="button" value="Delete"/>

Above is a screen view of the preconfigured services of the LoadMaster *Exchange* that you see when you click View/Modify Services. At the time of installation three of the above services will be shown with a status of Down (red color). These services will continue to show as Down until each service is configured with correct IP addresses at which time they status should change to Up and green color.

Each of the preconfigured Virtual Services are briefly described below.

RPC Client Access Service

The RPC Client Access (RPC CA) service is enabled by default when you install the Exchange 2010 Client Access Server role. The RPC CA service handles the Outlook MAPI connections.

The change in Exchange 2010 to move all processing to the Client Access Server was implemented to provide all data access through a single, common path of the Client Access Server. This change improves consistency for applying business logic to clients, and provides a better client experience when failover occurs. This change also allows a higher number of concurrent connections per server and a higher number of mailboxes per server.

Hub-Edge-SMTP

In Microsoft Server 2010, the Edge Transport server role is deployed in your organization's perimeter network. Designed to minimize the attack surface, the Edge Transport server handles all Internet-facing mail flow, which provides SMTP relay and smart host services for the organization. Additional layers of message protection and security are provided by a series of agents that run on the Edge Transport server and act on messages as they're processed by the message transport components. These agents support the features that provide protection

against viruses and spam and apply transport rules to control message flow.

Enforce Secure Access

With this service LoadMaster *Exchange* will autonomously redirect any unencrypted HTTP requests to an identical secured HTTPS connection.

All HTTPS Services

This is a catch-all service that provides application aware access for OWA, OA, EAS, ECP, EWS and AutoD services.

If you will be providing all services via a single FQDN you can install a simple single SSL certificate to provide security for all connections. Alternatively, you can provide these services on distinct FQDN's by installing a UCC (multi-named) certificate and setting DNS resolution for all FQDN's to the same virtual IP address.

To add further Exchange 2010 services, please refer to the Exchange 2010 configuration guide at: http://www.kemptechnologies.com/fileadmin/content/downloads/documentation/5.1/KEMP_Exchange_2010_Deployment_Guide_5_1.pdf.