



# LoadMaster *Exchange*

## Installation and Configuration Guide

Release 5.1.74

Updated: August 2011

### World Headquarters

KEMP Technologies Inc.  
12 Old Dock Road  
Yaphank, NY 11980  
U.S.A.

+1 631.345.5292

### EMEA Headquarters

KEMP Technologies Ltd.  
Mary Rosse Centre  
Holland Road, National Tech. Park  
Limerick, Ireland

+353 (61) 260 101

[www.kemptechnologies.com](http://www.kemptechnologies.com)

© 2002-2011 KEMP Technologies, Inc. All rights reserved. KEMP Technologies and the KEMP Technologies logo are registered trademarks of KEMP Technologies, Inc..

KEMP Technologies, Inc. reserves all ownership rights for the LoadMaster product line including software and documentation. The use of the LoadMaster appliance is subject to the license agreement. Information in this guide may be modified at any time without prior notice.

Microsoft Windows and Microsoft Client Access Server are registered trademarks of Microsoft Corporation in the United States and other countries. All other trademarks and service marks are the property of their respective owners.

**Limitations:** This document and all of its contents are provided as-is. KEMP Technologies has made efforts to ensure that the information presented herein are correct, but makes no warranty, express or implied, about the accuracy of this information. If any material errors or inaccuracies should occur in this document, KEMP Technologies will, if feasible, furnish appropriate correctional notices which Users will accept as the sole and exclusive remedy at law or in equity. Users of the information in this document acknowledge that KEMP Technologies cannot be held liable for any loss, injury or damage of any kind, present or prospective, including without limitation any direct, special, incidental or consequential damages (including without limitation lost profits and loss of damage to goodwill) whether suffered by recipient or third party or from any action or inaction whether or not negligent, in the compiling or in delivering or communicating or publishing this document.

## Table of Contents

<b>Table of Contents .....</b>	<b>3</b>
<b>1. About KEMP Technologies .....</b>	<b>5</b>
Load Balancing Microsoft Server 2010.....	5
About This Manual.....	6
Prerequisites .....	6
<b>2. Exchange 2010 Overview.....</b>	<b>7</b>
Understanding Server Load Balancing .....	7
Advantages to using a KEMP LoadMaster Exchange .....	8
KEMP LoadMaster Exchange - Optimized for Exchange 2010 .....	8
SSL Acceleration (SSL Offloading).....	8
L7 Transparency.....	9
Persistence .....	10
Idle Connection Timeout .....	10
Port 10	
Connection Scaling.....	10
Header Rewriting .....	10
<b>3. Load Balancing Client Access Server Services .....</b>	<b>11</b>
Full WUI Menu Tree .....	13
1 Home.....	14
2 Virtual Services .....	15
2.1 Add New VS .....	15
2.2 View/Modify Existing VS (HTTP Service Type) .....	15
2.3 View/Modify Existing (HTTP/HTTPS Service Type) .....	21
2.4 View/Modify Existing (Remote Terminal Service Type).....	23
2.5 Real Server Assignment.....	24
2.6 Add / Modify Real Server.....	24
3 Statistics .....	25
3.1 Global Statistics .....	25
3.2 Real Server Metrics .....	25
3.3 Virtual Service Metrics.....	26
4 Real Servers.....	27
5 Rules & Checking.....	28
5.1 Content Rule Management .....	28
5.2 Adaptive Parameters.....	29
5.3 Service (Health) Check Parameters .....	30
6 Certificates.....	31
6.1 Installed Intermediate Certificates.....	31
6.2 Certificate Signing Request .....	31
6.3 Installing Intermediate Certificates .....	32
6.4 Backing Up and Restoring Certificates .....	32
7 System Configuration .....	34
7.1 Interfaces.....	34
7.2 Local DNS Configuration .....	35
7.3 Route Management.....	35
7.4 Access Control .....	35
7.5 System Administration .....	36
7.6 Logging Options.....	39
7.7 Miscellaneous Options.....	42

<b>4. Appendix .....</b>	<b>50</b>
A. Persistence Table.....	50
B. Connection Scaling For Large Scale Deployments .....	51
C. Configuration Table .....	52
<b>5. Glossary.....</b>	<b>53</b>
<b>6. Index.....</b>	<b>54</b>
<b>7. Document History .....</b>	<b>55</b>

## 1. About KEMP Technologies

Since the year 2000, and with thousands of customers world-wide, KEMP leads the industry in driving the price/performance value proposition for application delivery and server load balancing to levels that businesses of any size can afford. KEMP's LoadMaster family of purpose-built hardware and Virtual Appliances (VLM) offer advanced L4/7 server load balancing, content switching, SSL Acceleration and a multitude of other advanced Application Delivery and Optimization (ADC) features. The LoadMaster intelligently and efficiently distributes user traffic among application servers so that your users get the best experience possible.

### Load Balancing Microsoft Server 2010

The big changes Microsoft has made to its core server architecture in 2010 create exciting new opportunities to manage the server infrastructure for always-on reliability and cluster-enabled application acceleration. Most important of these is Microsoft's 2010 strategy to emphasize scale-out, rather than scale-up, making the right load balancing solution more critical than ever. Now that Client Access Server (CAS) is used to handle all client connections, there's a well-defined endpoint for managing the delivery of an optimal user experience.

The KEMP LoadMaster Exchange combines versatility with ease-of-use to speed deployment of the complete portfolio of advanced messaging applications and protocols used by Exchange 2010, including Outlook Web App (OWA), Outlook Anywhere (OA), ActiveSync (EAS), Simple Mail Transfer Protocol (SMTP), Post Office Protocol version 3 (POP3), Internet Message Access Protocol version 4 (IMAP4) and RPC Client Access (RPC CA). With built-in SSL acceleration and/or overlay, the LoadMaster Exchange offloads a key source of CPU drain to improve the capacity of Client Access Servers. Layer 7 health checking at the LoadMaster Exchange ensures that should one of the servers become inaccessible, the load balancer will take that server off-line, while automatically re-routing and reconnecting users to other functioning servers.

The entire KEMP LoadMaster product family, including the Virtual LoadMaster (VLM) supports Microsoft Exchange 2010, and includes a comprehensive first year warranty and technical support agreement.

For more information about KEMP Technologies, visit us online at [www.kemptechnologies.com](http://www.kemptechnologies.com) or call +1 (631) 345-5292.

## About This Manual

This manual addresses how to deploy and configure a LoadMaster Exchange appliance with Microsoft Exchange 2010. Specifically, configuration information applies to the array of Exchange 2010 services.

Images used in this manual are samples to help you determine if you are “in the right place” when performing the configuration and may not be totally representative of what your screen may look like.

Certain procedures contain instructions that refer to a website. If you are configuring your LoadMaster Exchange at the same time that you need to access a website then you should access that site in a different browser session (i.e. do not use your web browser to access/configure the LoadMaster Exchange and then prior to finishing your configuration browse to a different URL and then use the “Back” button or other method to return to the LoadMaster Exchange).

## Prerequisites

It is assumed that the reader is a network administrator or otherwise familiar with IP networking and general computer terminology. It is further assumed that you have set up your Exchange 2010 environment and have installed your KEMP LoadMaster Exchange appliance.

You should have reviewed the KEMP LoadMaster QuickStart Guide (5.1), available at <http://www.kemptechnologies.com/documentation>.

At a minimum, you should have:

- Installed your Microsoft Servers, Active Directories and followed other Microsoft requirements.
- Installed LoadMaster Exchange on the same network as the Microsoft Servers.
- Established access to the LoadMaster Exchange Web User Interface.
- Recommended: changed the default gateway on the Real Servers to point to the LoadMaster Exchange. Doing so will allow accurate server-side access logging of client IP addressing.
- Created a Client Access array using the “New-ClientAccessArray”cmdlet (see steps at <http://technet.microsoft.com/en-us/library/ee332317.aspx>).

## 2. Exchange 2010 Overview

Microsoft Server Exchange 2010 provides several solutions for switchover and failover redundancy. These solutions include the following:

**High availability and site resilience:** You have the option of deploying two Active Directory sites in separate geographic locations or stretch a single AD site between the two locations, keep the mailbox data synchronized between the two, and have one of the sites take on the entire load if the other fails.

**Online mailbox moves:** In an online mailbox move, end users can access their e-mail accounts during the move. Users are only locked out of their accounts for a brief time at the end of the process, when the final synchronization occurs. Online mailbox moves are supported between Exchange 2010 databases and between Server 2007 Service Pack 2 (SP2) and Exchange 2010 databases. You can perform online mailbox moves across forests or in the same forest.

**Shadow redundancy:** Shadow redundancy protects the availability and recoverability of messages while they're in transit. With shadow redundancy, the deletion of a message from the transport databases is delayed until the transport server verifies that all the next hops for that message have completed. If any of the next hops fail before reporting successful delivery, the message is resubmitted for delivery to the hop that didn't complete.

For more information please refer to Microsoft documentation on this subject, available at <http://technet.microsoft.com/en-us/exchange/dd203064.aspx>.

### Understanding Server Load Balancing

Server load balancing is a way to manage which of your servers receive traffic. Server load balancing provides failover redundancy to ensure your users continue to receive service in case of failure. It also enables your deployment to handle more traffic than one server can process while offering a single host name for your clients.

Server load balancing serves two primary purposes. It reduces the impact of a single Client Access Server failure within one of your Active Directory sites. In addition, server load balancing ensures that the load on your Client Access Server and Transport servers is optimally distributed.

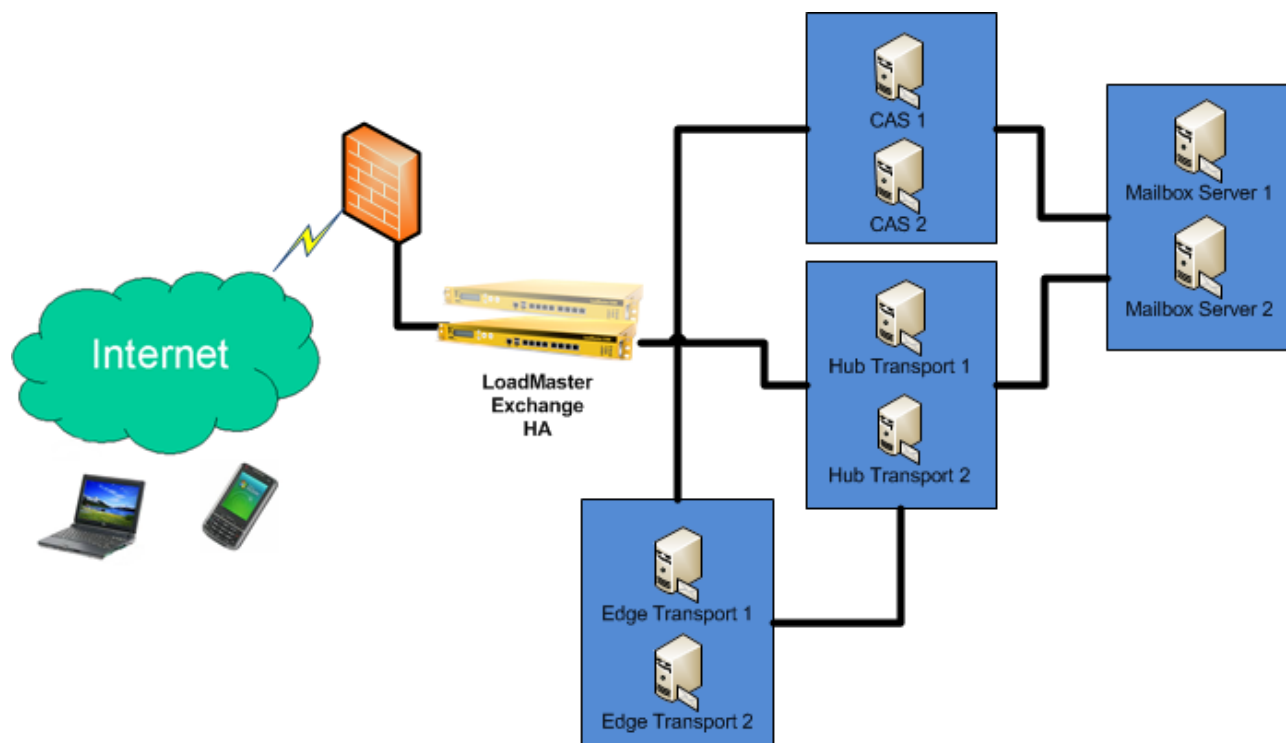
Server load balancing reduces the impact of a single Client Access Server failure within one of your Active Directory sites and ensures that the load on your Servers is evenly distributed. Architectural changes with respect to earlier versions of make server load balancing even more important than in the past. A load-balanced array of Client Access Servers is recommended for each Active Directory site and for each version of . It isn't possible to share one load-balanced array of Client Access Servers for multiple Active Directory sites or to mix different versions of or service pack versions of within the same array.

Several changes in Exchange 2010 make server load balancing important for your organization. The RPC Client Access Service on the Client Access Server role improves the user's experience during Mailbox failovers by moving the connection endpoints for mailbox access from Outlook and other MAPI clients to the Client Access Server role instead of to the Mailbox server. In earlier versions of , Outlook connected directly to the Mailbox server hosting the user's mailbox, and directory connections were either proxied through the Mailbox server role or referred directly to a particular Active Directory global catalog server. Now that these connections are handled by the Client Access Server role, both external and internal Outlook connections must be load balanced across the array of Client Access Servers in a deployment to achieve fault tolerance and optimal performance.

For more information, please refer to Microsoft documentation on this subject matter available on the Web at <http://technet.microsoft.com/en-us/library/ff625247.aspx> .

## Advantages to using a KEMP LoadMaster Exchange

KEMP LoadMaster Exchange offers performance, security and functional advantages that combine versatility with ease-of-use to speed deployment of the complete portfolio of advanced messaging applications and protocols used by Exchange 2010, including Outlook Web App (OWA), Outlook Anywhere (OA), ActiveSync (EAS), Simple Mail transfer Protocol (SMTP), Post Office Protocol 3 (POP3) and Internet Message Access Protocol (IMAP) and RPC Client Access (RPC CA). With built-in SSL acceleration and/or overlay, the LoadMaster offloads a key source of CPU drain to improve the capacity of Client Access Servers. Layer 7 health checking at the LoadMaster ensures that should one of the servers become inaccessible, the LoadMaster will take that server off-line, while automatically re-routing and reconnecting users to other functioning servers.



When a KEMP LoadMaster Exchange based CAS array has been configured, all servers in the array can be represented by a single VIP address and a FQDN. When a client request comes in, it will be sent to an Exchange 2010 CAS server in the CAS array using any available KEMP LoadMaster scheduling (distribution) method that you select. The scheduling method is defaulted to Round Robin as the preferred method because it does a better job of balancing traffic in many situations.

## KEMP LoadMaster Exchange - Optimized for Exchange 2010

Your KEMP LoadMaster Exchange has many features and capabilities that can be used to optimize the load balancing configuration to work best with your Exchange 2010 server load balancing requirements.

### SSL Acceleration (SSL Offloading)

The KEMP LoadMaster Exchange offers SSL acceleration (also referred to as “SSL offloading”) for Virtual Services. With SSL acceleration, the SSL session is terminated at the LoadMaster Exchange. Some of the benefits to using SSL acceleration are that the LoadMaster Exchange migrates the SSL workload from the Real Servers (which can be hardware accelerated by LoadMaster Exchange), can perform Layer 7 processing (such as Super HTTP -based persistence

or content switching), SSL security hardening, and a central point of management of SSL certificates.

With SSL Acceleration, the SSL session is terminated at the LoadMaster Exchange and sent to the Real Servers un-encrypted. In some security situations, it may be necessary to encrypt the connection between the LoadMaster Exchange and Real Servers. This can be achieved with reverse SSL. Review the LoadMaster Exchange manual to configure a reverse SSL deployment.

With reverse SSL, the SSL session is first terminated at the LoadMaster Exchange. Super HTTP persistence and other Layer 7 functionality can then be performed. After that, the traffic is re-encrypted in a new SSL session between the LoadMaster Exchange and the Real Server.

Without terminating the SSL session at the LoadMaster Exchange, the headers and content cannot be read, so Super HTTP persistence cannot be done. The only consistently reliable persistence method available when the SSL session is not terminated at the LoadMaster Exchange is Source IP.

Hardware SSL and Software SSL are the two types of SSL termination capabilities available in your LoadMaster Exchange. Functionally, hardware and software SSL are the same. The difference is in what part of the LoadMaster Exchange handles the actual cryptographic functions associated with SSL operations.

With software SSL, the LoadMaster Exchange's general processor handles encryption/decryption tasks. These tasks are shared with other tasks that the LoadMaster Exchange performs, such as server load balancing, health checking, and other administrative tasks. Because SSL operations are CPU-intensive, software SSL is sufficient for low levels of SSL traffic but insufficient for higher levels of SSL traffic. Higher connection rates of SSL on a software SSL LoadMaster Exchange may degrade overall performance of the LoadMaster Exchange.

With hardware SSL, the LoadMaster Exchange has a separate specialized processor, which handles all SSL functions. No matter the level of SSL connections, the LoadMaster Exchange's general processor is not burdened. This specialized hardware is purpose-built for SSL, and can handle extremely high connection rates (TPS) of SSL traffic.

An SSL certificate is required for all SSL transactions, and as such is required for all SSL-enabled Virtual Services. With the LoadMaster Exchange, there are two types of SSL certificates: self-signed certificates generated by the LoadMaster Exchange or the administrator and certificates that are signed by a trusted CA (Certificate Authority) such as Digicert, Verisign or Thawte. In addition, with LoadMaster Exchange you are managing only one certificate instead of multiple certificates on each Real Server.

When an SSL-enabled Virtual Service is configured on the LoadMaster Exchange, a self-signed certificate is installed automatically. Both self-signed and CA signed certificates provide encryption for data in motion. A CA-signed certificate also provides authentication -- a level of assurance that the site is what it reports to be, and not an impostor.

The primary operational difference between a self-signed certificate and a CA certificate is that with a self-signed, a browser will generally give some type of warning that the certificate came from an untrusted issuer. Generally, self-signed certificates should not be used for public-facing production websites. As such, the Exchange 2010 configuration instructions indicate that you would first need to export an appropriately signed certificate from Exchange 2010 in order that you may import it into the LoadMaster Exchange.

## **L7 Transparency**

Newly created Virtual Services on a LoadMaster Exchange are set to transparent by default. In transparent mode, the LoadMaster Exchange will forward traffic towards an Exchange 2010 CAS Server or Edge Transport Server while retaining the source IP address with which it arrived at the

LoadMaster Exchange. Transparency is important in Exchange 2010 deployments to avoid redundant re-authentication of client sessions.

For L7 transparency to work properly:

a) The Real Server settings must ensure that all server replies to client requests are routed through the LoadMaster Exchange. Typically, this is achieved by making the LoadMaster Exchange the Real Server's default gateway.

b) No clients may be located in the same IP subnet with the Real Servers. If necessary, you can use additional ports on the LoadMaster Exchange to ensure that Real Servers and Clients are located on distinct IP subnets.

Providing that just the first condition above is met, in a L7 transparent single arm configuration (with Virtual Servers and Real Servers on the same subnet), all clients will be able to still achieve end-to-end connectivity. However, those clients located on the same subnet (and ONLY those clients) will be handled non-transparently, and may experience redundant re-authentication prompts. Virtual Services operating on L4 always act transparently, but end-to-end connectivity will NOT be possible for same-subnet clients.

## Persistence

Session persistence (a.k.a. Session Affinity or Stickiness) is the ability of the LoadMaster Exchange to make sure a given Client always gets to the same Real Server, even across multiple connections. Persistence can make sure that all requests from a client are sent to the same server in a Server Load Balancer (SLB) array or server farm (in case of CAS array).

## Idle Connection Timeout

For each Virtual Service you can set idle connection timeout values for the TCP/IP connections. In order to make optimal use of your KEMP LoadMaster Exchange you should not set these timeout values too high, but also be careful not to set them too low as this could result in clients needing to reestablish a TCP/IP connection, which typically results in the end user will be informed to re-authenticate. It is recommended you test which timeout values works best in your specific scenario before the solution goes into production.

## Port

There are many different types of possible data paths. It is recommended that your port configuration stay within the realm of default protocol RFC. However, your KEMP LoadMaster Exchange may be configured to use whichever port happens to be most appropriate for your particular network. For more information regarding port definitions, refer to Microsoft documentation at <http://technet.microsoft.com/en-us/library/bb331973.aspx>.

## Connection Scaling


LoadMaster Exchange is a scalable load balancer, allowing for more than 64,000 client connections to a single Virtual Service at one time. If this is required, you should execute the Connection Scaling for Large Scale Deployments procedure located in the Appendix of this manual.

## Header Rewriting

Your KEMP LoadMaster Exchange offers HTTP header insertions, deletions, and modifications. Our header rewriting feature can be useful with respect to the URL users must input or remember. If you wish to use URL rewriting, you may wish to execute the Header Rewriting procedure located in the Appendix of this manual.

### 3. Load Balancing Client Access Server Services

This section how the KEMP LoadMaster Exchange is preconfigured for different services of the Exchange 2010 Client Access Server. The LoadMaster Exchange, Exchange 2010 services may be used as is, modified or deleted to suit your particular environment.

 The LoadMaster Exchange is preconfigured with thirteen (13) Virtual Services (VS), the maximum number allowed. Should there be a duplicate or additional service required, an existing service must be deleted.

Each service handled by the Client Access server role is briefly described below:

**Outlook Web App** Outlook Web App (OWA) is enabled by default when you install the Client Access server role. OWA lets you access your mailbox from a Web browser. In previous versions of , you needed to use a specific version of Internet Explorer in order to get the OWA premium experience. With Exchange 2010, you can get the premium experience with Microsoft Internet Explorer, Mozilla Firefox and Apple Safari.

**Control Panel:** The Control Panel (ECP) is enabled by default when you install the Client Access server role. ECP is a new web module that lets an end-user or administrator manage the miscellaneous settings or perform other tasks for an mailbox from a Web browser. It replaces the old OWA options page included with previous version of Server.

**Outlook Anywhere:** Outlook Anywhere (OA) feature, formerly known as RPC over HTTP, lets clients that use Microsoft Office Outlook 2010, Outlook 2007, or Outlook 2003 connect to their servers from outside the corporate network or over the Internet using the RPC over HTTP Windows networking component. The Windows RPC over HTTP Proxy component, which Outlook Anywhere clients use to connect, wraps remote procedure calls (RPCs) with an HTTP layer. This allows traffic to traverse network firewalls without requiring RPC ports to be opened. In Exchange 2010, as in 2007, it's easy to deploy and manage this feature. To deploy Outlook Anywhere (OA) in your Exchange 2010 messaging environment, you should enable OA on all Internet-facing Client Access Servers using the "Enable Outlook Anywhere wizard" in the Management Console or the "Enable-OutlookAnywhere" cmdlet. In addition, you must set the external URLs for ECP, EWS and OAB unless you're only public folders are used for distributing the OAB.

**ActiveSync:** ActiveSync (EAS) is enabled by default when you install the Client Access server role. ECP lets you synchronize a mobile phone with your Exchange 2010 mailbox. EAS is a Microsoft synchronization protocol that's optimized to work together with high-latency and low-bandwidth networks. The protocol, based on HTTP and XML, lets mobile phones access an organization's information on a server that's running Microsoft . EAS enables mobile phone users to access their e-mail, calendar, contacts, and tasks and to continue to be able to access this information while they're working offline.

**Offline Address Book:** The Offline Address Book (OAB) is created by default when you install the Mailbox server role. OAB is a copy of one or more address lists that's been downloaded so that an Outlook user can access the information it contains while disconnected from the server. administrators can choose which address lists are made available to users who work offline, and they can also configure the method by which the OAB is distributed (Web-based distribution or public folder distribution).

**Web Services:** The Web Services (EWS) is enabled by default when you install the Client Access server role. EWS is a web services application programming interface (API) that can be used by 3<sup>rd</sup> party applications to access mailbox data. It is also used by various Microsoft produced applications and devices for integration with .

**Autodiscover Service:** The Autodiscover Service (AS) is enabled by default when you install the Client Access server role. AS is a service that makes it easier to configure Outlook 2007 or

Outlook 2010 and EAS-based mobile devices that support this service. You can't use the Autodiscover service with earlier versions of Outlook, including Outlook 2003.

**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. In addition to moving processing of incoming Outlook connections to the Client Access Server, in Exchange 2010, directory access is also handled by the Client Access Server.

**Address Book Service:** The Address Book (EAB) service is enabled by default when you install the Exchange 2010 Client Access server role. The EAB service handles directory access requests from Outlook clients.

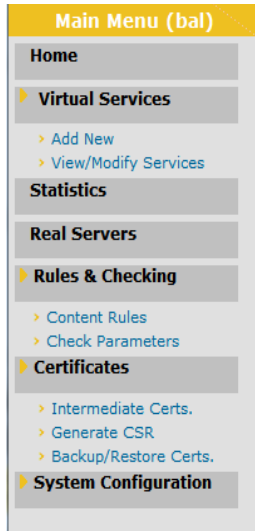
**Post Office Protocol:** Post Office Protocol (POP) is disabled by default when you install the Exchange 2010 Client Access server role. POP was designed to support offline mail processing. With POP3, e-mail messages are removed from the server and stored on the local POP3 client, unless the client has been set to leave mail on the server. This puts the data management and security responsibility in the hands of the user. POP3 doesn't offer advanced collaboration features such as calendaring, contacts, and tasks.

**Internet Message Access Protocol:** Internet Message Access Protocol (IMAP) is disabled by default when you install the Exchange 2010 Client Access server role. IMAP offers offline and online access, but like POP3, IMAP4 doesn't offer advanced collaboration features such as calendaring, contacts, and tasks.

## Full WUI Menu Tree




This section is Quick Reference that will help you find your way through the menu structure of the LoadMaster Exchange WUI.

The LoadMaster Exchange menu consists of a series of collapsible submenus on the left of the screen.



## 1 Home

An introduction page showing the vital information of the LoadMaster.


IP address	192.168.201.3
Machine Identifier	7E2K8YQRWUe4
Boot Time	Thu Aug 11 15:03:51 UTC 2011
LoadMaster Exchange Version	5.1-74.20110726-0654
License	Activation date: January 13 2011 Licensed until: Unlimited
CPU Load	0% 
TPS	Total 0 (SSL 0)
NetLoad	Mbits/sec
eth0	0.0 
eth1	0.0 

The CPU load and Net load data are updated every 5 seconds.

## 2 Virtual Services

A list of Virtual Services on the LoadMaster, summarizing the properties of each and giving the options to modify or delete existing services, or create a new service.

Virtual IP Address	Prot	Name	Layer	Certificate Installed	Scheduler	Status	Real Servers
1 10.0.1.84:*	tcp	RPC Client Access Service	L7		round robin	Up	<input type="button" value="Modify"/> <input type="button" value="Delete"/>
2 10.0.1.84:25	tcp	Hub-Edge-SMTP	L7		least connection	Up	<input type="button" value="Modify"/> <input type="button" value="Delete"/>
3 10.0.1.84:80	tcp	Enforce Secure Access	L7		round robin	Reirect	<input type="button" value="Modify"/> <input type="button" value="Delete"/>
4 10.0.1.84:443	tcp	All HTTPS Services -OWA OA EAS	L7	<input type="button" value="Add New"/>	round robin	Up	<input type="button" value="Modify"/> <input type="button" value="Delete"/>

 The LoadMaster *Exchange* is preconfigured with four (4) Virtual Services (VS) as shown above. The maximum number VS's allowed is thirteen (13).



**CAUTION** Once deleted, there is no UNDO feature to retrieve a VS. Use **DELETE** with care.






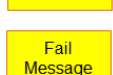
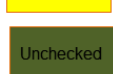
### 2.1 Add New VS

Here the Virtual IP (VIP) address, port and protocol are defined. The VIP address and port must be typed manually into the text fields and the protocol is selected from the pull-down list.

### 2.2 View/Modify Existing VS (HTTP Service Type)

Each configured Virtual Service may be changed by clicking the MODIFY button or deleted by clicking the DELETE button. Here the properties of the Virtual Services are shown, and may be modified.

The Virtual Service status may be one of the following:

	Up – At least one Real Server is available.
	Down – No Real Servers are available.
	Sorry – All Real Servers are down and traffic is routed to a separately configured server, not part of the Real Server set, with no checking.
	Disabled – The service has been administratively disabled.
	Redirect – A fixed redirect response has been configured.
	Fail Message – A fixed error message has been configured.
	Unchecked – The User has disabled checking of the Real Servers. All RS are accessed and presumed UP.


The image below shows a complete screen for a Virtual Service. It is composed of four sections:

**Basic Properties** - where the usual and most common attributes are set..

**SSL Properties** – if SSL acceleration (server SSL offloading) is being used, this section of the screen will be used to configure the functions.

**Advanced Properties** – the additional features for Virtual Services.

**Real Servers** – the server(s) to which the VS will connect.

 Depending upon the service type, only specific fields and options are shown in the screen captures in this document and the screens may not represent every possible configuration.

Detailed description of each section of the screen is given below.

### ***Activate or Deactivate Service***

This checkbox gives you the option to activate or deactivate a Virtual Service. The default is checked - active.

### ***Service Type***

Setting this controls the options displayed for the Virtual Service. Its important to make sure the Service Type is set according to the type of application you are load balancing.



### ***Port Range***

You may specify a sequential range of ports, starting with the base port already configured for the Virtual Service. The maximum range is 1,024 ports. Therefore, if the base port is 80, then the maximum value in this field is 1,104.

### ***Extra Ports***

If a range does not suit your needs, you may specify individual ports, up to a maximum of 256. The port numbers are inputted to the field and separated with a space. No ranges may be included –they must all be single port numbers, even if they are consecutive.



Port Range and Extra Ports are mutually exclusive and not applicable to a VS with a 443 port.

### ***Force L7***

If visible, the Force L7 should be checked (default). If it is unchecked it will force the Virtual Service to Layer 4.

### ***L7 Transparency***

Enabling this option makes the Virtual Service transparent (NO NAT). However, If the client resides on the same subnet as the Virtual IP and Real Servers the Virtual Services will automatically NAT (enable non-transparency) the source IP.

### ***Allow Server Initiating Protocols***

By default, the LoadMaster will not initiate a connection to a Real Server until it has received some data from the client. This can cause problems for certain protocols - SSH and SMTP are two notable examples. Enabling this option will force the immediate connection the Real Server to allow these protocols to work correctly

**Properties for 192.168.201.31:443 - Operating at Layer 7**

<<Back
**Basic Properties**
Duplicate VIP
Change Address

Activate or Deactivate Service	<input checked="" type="checkbox"/>
Service Type	HTTP/HTTPS ▾
L7 Transparency	<input checked="" type="checkbox"/>
Real Server Check Parameters	HTTP Protocol ▾ Checked Port <input type="text"/> <span>Set Check Port</span>
	URL: <input type="text" value="/owa"/> <span>Set URL</span>
	Use HTTP/1.1: <input type="checkbox"/>
	HTTP Method: HEAD ▾
Service Nickname	All HTTPS Services -OWA OA <span>Set Nickname</span>
Persistence Options	Mode: Super HTTP ▾
	Timeout: 1 Hour ▾
Scheduling Method	round robin ▾
Idle Connection Timeout	900 <span>Set Idle Timeout</span>
Use Address for SNAT	<input type="checkbox"/>

**SSL Properties**

SSL Acceleration	Enabled: <input checked="" type="checkbox"/> Reencrypt: <input type="checkbox"/>
Certificates	Self Signed Certificate in use: <span>Add New</span> <span>Add Intermediate Cert</span>
Rewrite Rules	None ▾
Client Certificates	No Client Certificates required ▾

**Advanced Properties**

Content Switching	Disabled <span>Enable</span>
HTTP Header Modifications	<span>Show Header Rules</span>
Enable Caching	<input checked="" type="checkbox"/> Maximum Cache usage 90% ▾ Current usage assigned 90%
Enable Compression	<input checked="" type="checkbox"/>
Detect Malicious Requests	<input checked="" type="checkbox"/> Intrusion Handling Drop Connection ▾ Warnings <input type="checkbox"/>
Add Header to Request	FRONT-END-HTTP: ON <span>Set Header</span>
Not Available Server	<input type="text"/> <span>Set Server Address</span>
Not Available Redirection Handling	Error Code: <input type="text"/>
	Redirect URL: <input type="text"/> <span>Set Redirect URL</span>
Add a Port 80 Redirector VS	Redirection URL: https://%h%s <span>Add HTTP Redirector</span>
Default Gateway	<input type="text"/> <span>Set Default Address</span>

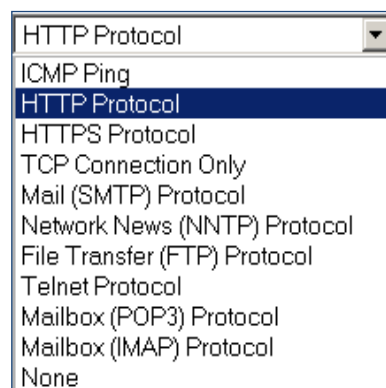
**Real Servers for this Virtual Service**

Add New ...

	Operation	IP Address	Port	Forwarding method	Weight	Status
<span>Disable</span> <span>Modify</span> <span>Delete</span>		192.168.201.35	80	nat	1000	Enabled
<span>Disable</span> <span>Modify</span> <span>Delete</span>		192.168.201.36	80	nat	1000	Enabled

### **Real Server Check Parameters**

This provides a list of checks for well-known services, as well as lower level checks for TCP/UDP or ICMP. With the service checks, the Real Servers are checked for the availability of the selected service. With TCP/UDP the check is simply a connect attempt.



### **Healthcheck URL**


By default, the health checker tries to access the URI / to determine if the machine is available. A different URL can be specified here.

### **HTTP Healthcheck Method**

When accessing the healthcheck URL, the system can use either the HEAD or the GET method.

### **HTTP Reply 200 Pattern**

When using the GET method, the contents of the returned response message can be checked. If the response contains the string specified by this Regular Expression, then the machine is determined to be up. (The response will have all HTML formatting information removed before the match is performed. Only the first 4K of response data can be matched.

 If the pattern starts with a caret '^' symbol, it inverts the pattern response.

The following health-check methods may be specified.

<b><u>Method</u></b>	<b><u>Action</u></b>
ICMP Ping	An ICMP ping is sent to the Real Server
HTTP	HTTP checking is enabled
HTTPS	HTTPS (SSL) checking is enabled
TCP	A basic TCP connection is checked.
Mail	The SMTP (Simple Mail Transfer Protocol) is used.
NNTP	The (Network News Transfer Protocol) is used.
FTP	The (File Transfer Protocol) is used.
Telnet	The (Telnet protocol) is used.
POP3	The (Post Office Protocol – mail client protocol) is used.
IMAP	The (Internet Message Access Protocol – mail client protocol) is used.
None	No checking performed.

### **Service nickname**

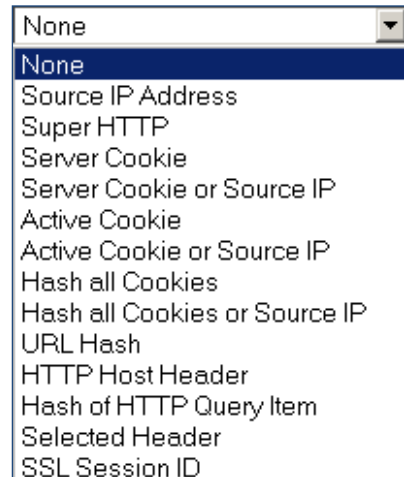
This text field allows you to assign a nickname to the Virtual Service being created, or change an existing one.

### **Persistence Options**

This section allows you to select whether persistence is enabled for this service, to set the type of persistence and the persistence timeout value.

If persistence is enabled it means that a client connection to a particular Real Server via the balancer is persistent, in other words the same client will subsequently connect to the same Real Server. The timeout value determines for how long this particular connection is remembered.

The pull-down list gives you the option to select the type of persistence. These are:



#### **Source IP Address**

The source IP address (of the requesting client) is used as the key for persistency in this case. The netmask+ determines how the Balancer sees a 'client' in the context of persistence. For example:

When the netmask is set to 255.255.255.255 (the default) then every individual IP address qualifies as a valid persistent context. So, a client with the IP address 200.190.125.67 connects, and its connection to a particular Real Server is remembered. The client then ends the session and disconnects. A short time later, the client begins another session, but this time its IP address is given as 200.190.125.44 - it will not necessarily be directed to the same Real Server as before.

However, using the example above, if the netmask is set to 255.255.255.0, then all clients connecting with an IP address of 200.190.125.X will be grouped together and directed to the same Real Server, until the timeout has expired.

#### **Super HTTP**

The balancer checks the value of the User-Agent header and the Authorization header, if present. Connections with the same header combination will go to the same Real Server.

#### **Server Super HTTP**

The Balancer checks the value of a specially set Super HTTP in the HTTP header. Connections with the same Super HTTP will go to the same Real Server.

#### **Server Super HTTP or Source IP**

If Super HTTP persistence fails, it reverts to source-based persistence.

#### **Active Super HTTP**

The Balancer automatically sets the special Super HTTP .

#### **Active Super HTTP or Source IP**

If active Super HTTP persistence fails, it reverts to source-based persistence.

#### **Hash All Super HTTP s**

The Hash All Super HTTP s method creates a hash of the values of all Super HTTP s in the HTTP stream. Super HTTP s with the same value will be sent to the same server for each request. If the values change, then the connection will be treated as a new connection, and the client will be to a server according to the load balancing algorithm.

### **Hash All Super HTTP s or Source IP**

Hash All Super HTTP s or Source IP is identical to Hash All Super HTTP s, with the additional feature that it will fall back to Source IP persistence in the event no Super HTTP s are in the HTTP string.

### **Host Persistence**

A request to the same host always goes to the same server.

### **URL Hash**

With URL Hash persistence, the LoadMaster will send requests with the same URL to the same server.

### **HTTP Host Header**

With HTTP Host Header persistence, the LoadMaster will send all requests that contain the same value in the HTTP Host: header to the same server.

### **Hash of HTTP Query Item**

This method operates in exactly the same manner as Server Super HTTP Persistence, except that the named item being inspected is a Query Item in the Query String of the URL. All queries with the same Query Item value will be sent to the same server.

### **Selected Header**

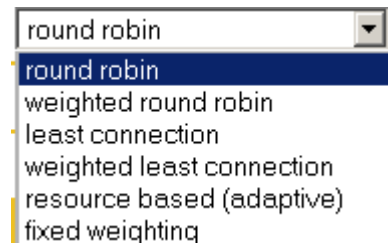
With Selected Header persistence, the LoadMaster will send all requests that contain the same value in the specified header to the same server.

### **SSL Session ID**

The SSL session ID is used to keep a session connected to the same server. Note: SSL acceleration must be disabled with this method.

### **Scheduling method**

This section allows you to select the method by which the balancer will select a Real Server, for this particular service. The scheduling methods are as follows:



#### **Round Robin**

Round Robin causes the balancer to assign Real Servers to a session in order, i.e. the first session connects to Real Server 1, the second to Real Server 2 etc. There is no bias in the way the Real Servers are assigned.

#### **Weighted Round Robin**

This method uses the weight property of the Real Servers to determine which Real Servers get preference. The higher the weight a Real Server has, the higher the proportion of connections it will receive.

#### **Least Connection**

With this method, the current Real Server with the fewest open connections is assigned to the session.

### **Weighted Least Connection**

As with Least Connection, but with a bias relative to the weight.

### **Resource Based (Adaptive)**

Adaptive scheduling means that the load on the Real Servers is periodically monitored and that packets are distributed such that load will be approximately equal for all machines. More details can be found in the section covering scheduling methods.

### **Fixed Weighting**

All traffic goes to highest weight RS that is available. Real Servers should be weighted at the time they are create and no two RS' should have same weight otherwise led unpredictable results may occur.

Idle Connection Timeout - . if there is no traffic for the period of time specified the connection is timed out and disconnected. The default is 11 minutes.

Use Address for SNAT - If not enabled transaction will show as originating from the address of the originating LoadMaster. When enabled a transaction shows the address of the VS. This is particularly used for SMTP.

### **SSL Acceleration**

This checkbox appears when the criteria for SSL Acceleration have been met, and serves to activate SSL Acceleration. If there is no certificate for the Virtual Service, you will be prompted to install a certificate. To download a certificate, enter the remote host where the certificate is located and your username and password for this host. Then enter the filename of the certificate and the private key, and click "Get File" to install them.

SSL Properties	
SSL Acceleration	Enabled: <input checked="" type="checkbox"/>
Certificates	Self Signed Certificate in use: <input type="button" value="Add New"/> <input type="button" value="Add Intermediate Cert"/>
Rewrite Rules	None
Client Certificates	No Client Certificates required

### **Certificates**

You may add a new certificate or add an intermediate certificate chain to the LoadMaster.

### **Rewrite Rules**

When the Real Server rejects a request with an HTTP redirect, the resulting Location URL may need to be converted to specify HTTPS instead of HTTP (and vice-versa).

### **Client Certificates**

This option should not be changed from the default of No Client Certificates required.. You would only use this feature if you are sure that all clients that access this service have valid client certificates.

## **2.3 View/Modify Existing (HTTP/HTTPS Service Type)**

Properties of the Virtual Service include the Generic Type and also provide HTTP/HTTPS specific options.

### **Advanced Properties**

## Content Switching

Enable Rule based Content switching on this Virtual Service. Once enabled, rules must be assigned to the various Real Servers. Rules can be attached to Real Server by selecting the “None” button located next the Real Server. Once rules are attached to a Real Server the “None” button will display the count of rules attached.

Advanced Properties	
Content Switching	Enabled
HTTP Header Modifications	Show Header Rules
Enable Caching	<input type="checkbox"/>
Enable Compression	<input type="checkbox"/>
Detect Malicious Requests	<input type="checkbox"/>
Not Available Server	<input type="text"/> Set Server Address
Not Available Redirection Handling	Error Code: <input type="text"/> Redirect URL: <input type="text"/> Set Redirect URL
Add a Port 80 Redirector VS	Redirection URL: <input type="text"/> Add HTTP Redirector
Default Gateway	<input type="text"/> Set Default Address

## Rule Precedence

The order in which Content switching rules are matched are specified here. This option only appears when Content Switching is enabled. This contains a summary list of rules assigned to the Virtual Service in question.

Real Servers for this Virtual Service							
Add New ...							
Operation	IP Address	Port	Forwarding method	Weight	Status	Rules	
Disable Modify Delete	10.0.0.3	80	nat	1000	Enabled	4	
Disable Modify Delete	10.0.0.4	80	nat	1000	Enabled	None	

This shows the Real Servers configured and whether any rules have been assigned to them. In this example the first RS has two rules and by clicking the button marked ‘2’ brings up the screen below.

Rules assigned to Virtual Service 10.0.0.2:443						
Operation	Name	Match Type	Options	Header	Pattern	
	RL1	RegEx	Ignore Case		rules	
Promote	RL4	postfix	Ignore Case		kemp	
Promote	RL6	RegEx	Ignore Case		tech	
	default					

This screen shows the rules that are assigned to this Real Server and the order in which they apply. To re-order the rules they have to be deleted from the RS and then added back in the required processing order. A rule may be promoted in the order of precedence by clicking its corresponding “Promote” button.

## Enable Caching

Turns caching on for URL's.



Types of files that can be cached may be defined in AFE configuration under the Systems Configuration, Miscellaneous options menu.

### **Enable Compression**

Files sent from LoadMaster are compressed with Gzip.



If compression is enabled without caching, LoadMaster performance may suffer.



Types of files that can be compressed may be defined in AFE configuration under the Systems Configuration, Miscellaneous options menu.

### **Port Following**

Port following enables a switch from an HTTP connection to an HTTPS (SSL) connection to be persistent on the same Real Server. Port following can only be switched on if the current service is an HTTPS service, and if there exists a HTTP service with the same IP address as this HTTPS service. Both Virtual Services must have the same set of Real Servers and both Virtual Services should have a Layer 7 persistence enabled.

### **Not Available Server**

If no Real Servers are available, the LoadMaster will redirect to a specified location, with no checking. Colloquially referred to as the Sorry server.

### **Not Available Redirection Handling**

When no Real Servers are available to handle the request you can define the error code and URL that the client should receive.

#### **Error Code:**

If no Real Servers are available, the LoadMaster can terminate the connection with a HTTP error code. Select the appropriate error code.

#### **Set Redirect URL:**

When no Real Servers are available and an error response is to be sent back to the client, a Redirect URL can also be specified. The URL value can be parameterized. %h is used to substitute hostname and %s will substitute URI.

## **2.4 View/Modify Existing (Remote Terminal Service Type)**



This section is not relevant to the LoadMaster *Exchange* product.

Properties of the Virtual Service include the Generic Type and also provide Remote Terminal specific options.

### **Persistence**

If the terminal servers support a Session Directory, the LoadMaster will use the "routing token" supplied by the Session Directory to determine the correct host to connect to. The LoadMaster persistency timeout value is irrelevant here - it is a feature of the Session Directory.



The switch "IP address redirection" in the Session Directory configuration MUST be UNCHECKED for this to work.

Using Session Directory with LoadMaster is optional, in terms of persistence. If the Client pre-populates the username and password fields (see figure x) in the initial request, then this value is stored on the LoadMaster. As long as these fields are still populated upon reconnect, the

LoadMaster will look up the name and reconnect to the same server as the original connection. The persistence timeout is used to limit the time the information is kept on the LoadMaster.

If using "Terminal-Service or Source IP" mode, then if neither of these two modes succeeds, then the source IP address will be used for persistency.

### ***Service Check for the Virtual Service***

Only three options are available. ICMP, TCP and RDP. Remote Terminal Protocol opens a TCP connection to the Real Server on the Service port (port 3389). The LoadMaster sends a1110 Code (Connection Request) to the server. If the server sends a1101 Code (Connection Confirm) then LoadMaster closes the connection and marks the server as active. If the server fails to respond within the configured response time for the configured number of times or if it responds with a different status code, it is assumed dead.

## **2.5 Real Server Assignment**

This section lists the Real Servers that are assigned to the Virtual Service. The properties of the Real Servers are summarized and there is also the opportunity to add or delete a Real Server, or modify the properties of a Real Server. When Content Switching is enabled, there is also the opportunity to add rules to, or remove rules from, the Real Server (see Add Rule).

## **2.6 Add / Modify Real Server**

 For the LoadMaster *Exchange*, there is a limit of six (6) Real Servers that may be configured.

Here, the properties of the Real Server are set. These are:

The Real Server IP address (this is not editable when modifying a Real Server).

The forwarding port of the Real Server. This field is editable, so the port may be altered if necessary.

The forwarding method. This is NAT - Network Address Translation - or Route (Direct) forwarding – if available dependent on the other modes selected for the service.

The Real Server's weight. This is weight of the Real Server, as used by the Weighted Round Robin, Weighted Least Connection and Adaptive scheduling method. The default initial value for the weight is 1000, the maximum is 65535, the minimum is 1. It is a good benchmark to give a Real Server a weight relative to its processor speed, i.e. if server1 seems to bring four times the power of server2, assign a weight of 4000 to server1 and weight of 1000 to server2.

### 3 Statistics

Shows the activity for the Loadmasters within the system (Global), the Real Servers and the Virtual Services

#### 3.1 Global Statistics

##### CPU

This table displays the following CPU utilization information for a given Balancer:

Use                    the percentage of the CPU, which is spent in processing in user mode

System                the percentage of the CPU spent processing in system mode

I/O Waiting          the percentage of the CPU spent waiting for I/O to complete

Idle                    the percentage of CPU, which is idle

 The sum of these 4 percentages will = 100%

Core Temp          temperature for each CPU core is displayed for LoadMaster hardware appliances by clicking the link for each CPU. Temperature will not show on a Virtual LoadMaster statistics screen.



##### Memory

This bar graph shows the amount of memory in use and the amount of memory free on the balancer.

##### Network Activity

These bar graphs show the current network throughput on each interface.

#### 3.2 Real Server Metrics

These graphs display the connections, bytes or bits (depending on choice: the buttons in the top right of the page toggle which value is to be displayed) handled by each Real Server. The value is a sum over all Virtual Services that this Real Server is a part of, and is represented as a percentage of the overall value for the whole balancer.

Global **Real Servers** Virtual Services Connections Bytes Bits

	RS-IP	Status	Total Conns	Last 60 Sec	5 Mins	30 Mins	1 Hour	Active Conns	Current Rate Conns/sec	[%]	Conns/sec
1	<a href="#">192.168.201.35</a>	Down	0	0	0	0	0	0	0	0	
2	<a href="#">192.168.201.36</a>	Down	0	0	0	0	0	0	0	0	
2	<b>System Total Conns</b>		0	0	0	0	0	0	0 /sec		

### 3.3 Virtual Service Metrics


These graphs display the total number of connections, bytes or bits for each Virtual Service, and displays how these are distributed across the Virtual Service's Real Servers by means of the percentage of the total for the Virtual Service that each Real Server handles.

Global Real Servers **Virtual Services** Connections Bytes Bits


	Virtual IP Address	Protocol	Status	Total Conns	Last 60 Sec	5 Mins	30 Mins	1 Hour	Active Conns	Current Rate Conns/s	Real Servers	
											RS-IP	[%] Conns/s
1	<a href="#">192.168.201.30:*</a>	tcp	Down	0	0	0	0	0	0	0	<a href="#">192.168.201.35</a>	0
2	<a href="#">192.168.201.31:443</a>	tcp	Down	0	0	0	0	0	0	0	<a href="#">192.168.201.35</a>	0
											<a href="#">192.168.201.36</a>	0
3	<a href="#">192.168.201.32:80</a>	tcp	Redirect	0	0	0	0	0	0	0	<a href="#">192.168.201.36</a>	0
4	<a href="#">192.168.201.33:25</a>	tcp	Down	0	0	0	0	0	0	0	<a href="#">192.168.201.35</a>	0
4	<b>System Total Conns</b>			0	0	0	0	0	0	0 /sec		

## 4 Real Servers

	Real Server	Status	Operation	
1	10.0.0.1	Enabled	Enable	Disable
2	10.0.0.3	Enabled	Enable	Disable
3	10.0.0.4	Enabled	Enable	Disable

 There is a maximum limit of six (6) Real Servers that may be configured.

This screen shows the current status of the Real Servers and gives the user the option to Disable or Enable each RS. Each Real Server has a corresponding buttons, and pressing one button will take an online server offline, and vice-versa. The status can be Enabled (Green), Disabled (Red) or Partial (Yellow) –meaning the Real Server is enabled in one Virtual Service.

 **CAUTION:** disabling a Real Server will disable it for all Virtual Services configured to use it. If it is the only RS available, i.e. the last one, the VS will effectively be down and not pass any traffic.

## 5 Rules & Checking

### 5.1 Content Rule Management

This screen shows rules that have been configured and gives the option to Modify or Delete.

Content Matching Rules						
	Operation	Name	Match Type	Options	Header	Pattern
1	<input type="button" value="Modify"/> <input type="button" value="Delete"/>	RL1	RegEx	Ignore Case		rules
2	<input type="button" value="Modify"/> <input type="button" value="Delete"/>	RL2	prefix	Negate Add Host		1234

Header Modification Rules						
	Operation	Name	Rule Type	Header	Pattern	Replacement
3	<input type="button" value="Modify"/> <input type="button" value="Delete"/>	RL5	Add Header	TEST		rules

To define a new rule, click on "Create New". You must give the rule a name.



**Hint:** Rule names must be alphanumeric, unique, case sensitive and start with a character. Thus two different rules can exist in the form "Rule1" and "rule1"

Rule Name	<input type="text"/>
Rule Type	Content Matching ▾
Match Type	Regular Expression ▾
Header Field	<input type="text"/>
Match String	<input type="text"/>
Negation	<input type="checkbox"/>
Ignore Case	<input type="checkbox"/>
Include Host in URL	<input type="checkbox"/>
Include Query in URL	<input type="checkbox"/>



Giving a rule an existing name will overwrite the rule of that exact name.

For separate detailed documentation see:  
<http://www.kemptechnologies.com/fileadmin/content/downloads/documentation/5.1/Header-Modification-Guide.pdf>

Rule Types:

- Content Matching – matches the content of the header
- Add Header – adds a header according to the rule
- Del Header – deletes the header according to the rule
- Replace Header – replaces the header according to the rule
- Modify URL – changes the URL according to the rule

Match Types:

- Regular Expression – compares the header to the rule
- Prefix – compares the prefix of the header according to the rule
- Postfix – compares the postfix of the header according to the rule

These match to the URL as follows:

/absolute/pathname/of/the/url/foo.html  
 |-> Prefix                      Postfix ->|

|-> Regular Expression ->|

With the "**Include host in URL**" checkbox checked, the host name is also included in the URL match string:

www.a-host.com/absolute/pathname/of/the/url/foo.html

|-> Prefix Postfix ->|

|-> Regular Expression ->|

The protocol definition (e.g. http://) is ignored in all cases. Finally, enter the string that is to be matched. Prefix and Postfix use standard strings and match exactly to what is entered. Regular Expression uses the following syntax:

- ? - Match any single character
- \* - Match zero or more characters
- \$ - End of line
- ^ - Start of line
- [ - Start of set, of which only one character will be matched. Must be terminated by ]
  - ^ At start of a set matches a character not in the set.
- \ - Escapes the next character

## 5.2 Adaptive Parameters

**Adaptive Parameters**

Adaptive Interval (sec)	10 <input type="button" value="v"/>
Adaptive URL	<input type="text" value="/load"/> <input type="button" value="Set URL"/>
Port	80 <input type="button" value="Set Port"/>
Min. Control Variable Value (%)	5 <input type="button" value="v"/>

### 5.2.1 Adaptive Interval

This is the interval, in seconds, at which the balancer checks the load on the servers. A low value means the balancer is very sensitive to load, but this comes at a cost of extra load on the balancer itself. 7 seconds is a good starting value. This value must not be less than the HTTP checking interval.

### 5.2.2 Adaptive URL

The Adaptive method retrieves load information from the servers via an HTTP inquiry. This URL specifies the file where the load information of the servers is stored. The standard location is "/load". It is the servers' job to provide the current load data in this file in ASCII format. In doing so, the following must be considered:

An ASCII file containing a value in the range of 0 to 100 in the first line where:

0=idle and 100=overloaded. As the number increases, i.e. the server becomes more heavily loaded, the LoadMaster will pass less traffic to that server. Hence, it 'adapts' to the server loading.

The file is set to "/load" by default.

The file must be accessible via HTTP

The URL must be the same for all servers that are to be supported by the adaptive method

**Note:** This feature is not only of interest for HTTP based Virtual Services, but for all Services. HTTP is merely used as the transport method for extracting the application specific load information from the Real Server.

### 5.2.3 Port

The port number of the HTTP daemon on the servers. The default value is 80.

### 5.2.4 Min Control Variable Value

This value specifies a threshold below which the balancer will switch to static weight-based scheduling, i.e. normal Weighted Round Robin. The value is a percentage of the maximum load (0-50). The default is 5.

## 5.3 Service (Health) Check Parameters

The LoadMaster utilizes Layer 3, Layer4 and Layer7 health checks to monitor the availability of the Real Servers and the Virtual Services.

Service Check Parameters	
Check Interval(sec)	9
Connect Timeout (sec)	4
Retry Count	2
<input type="button" value="Reset values to Default"/>	

### 5.3.1 Check Interval

With this field you can specify the number of seconds that will pass between consecutive checks. The recommended value is 7 seconds.

### 5.3.2 Connect & Response timeouts

The HTTP request has two steps: contact the server, and then retrieve the file. A timeout can be specified for each step, i.e. how long to wait for a connection, how long to wait for a response. A good value for both is 3 seconds.

### 5.3.3 Re-try Count

This specifies the number of retry attempts the check will make before it determines that the server is not functioning. A value of 1 or less disables retries.

## 6 Certificates

All new certificates are generated with a 1024 bit key by default. If the the box marked Use 2048 bit key is clicked, an appropriate CSR is generated

### 6.1 Installed Intermediate Certificates

Shows a listing of the installed intermediate certificates and the name assigned to them.

**Intermediate Certificates currently installed on your LoadMaster**

File Name	Options
james.pem	<input type="button" value="Delete"/>
james1.pem	<input type="button" value="Delete"/>

### 6.2 Certificate Signing Request

If you do not have a certificate, you may complete the Certificate Signing Request (CSR) and click Create CSR button.

Create a Certificate Signing Request (CSR) Vers:5.1-45

**All Fields are optional except "Common Name"**

2 Letter Country Code (ex. US):	<input type="text"/>
State/Province (Entire Name - New York, not NY):	<input type="text"/>
City:	<input type="text"/>
Company:	<input type="text"/>
Organization (e.g., Marketing,Finance,Sales):	<input type="text"/>
Common Name: (The fully qualified domain name for your web server)	<input type="text"/>
Email Address:	<input type="text"/>
SAN/UCC Names	<input type="text"/>
Use 2048 bit key	<input type="checkbox"/>

After clicking the 'Create CSR' button, the following screen appears:





**CAUTION** This passphrase is a mandatory requirement to restore a certificate. A certificate cannot be restored without the passphrase. If it is forgotten, there is no way to retrieve it and a new backup must be created with a new passphrase.

**Certificate Backup**

Backup all VIP and Intermediate Certificates	Passphrase <input type="text"/>	<input type="button" value="Create Backup File"/>
--	---------------------------------	---

**Restore Certificates**

Backup File <input type="text"/> <input type="button" value="Browse..."/>	
Which Certificates <input type="text" value="What to restore"/>	<input type="button" value="Restore Certificates"/>
Passphrase <input type="text"/>	

## 7 System Configuration

This section provides access to the parameters of the LoadMaster and the systems as an entire entity and is shown on the lower left side of the screen.

### 7.1 Interfaces

Describes the external network and Internal network interfaces. The screen has the same information for the eth0 and eth1 Ethernet ports. The example below is for eth0 on a non HA unit. Also see VLAN bonding in Section O. If you have older infrastructure that does not support VLAN tagging, you may associate additional subnets to any interface by designating a base network address and a subnet mask. The LoadMaster will not create any routes to these additional subnets. If needed, an external device supporting router-on-a-stick configuration can be deployed alongside the LoadMaster.

**Network Interface 0**

Interface Address (xx.xx.xx.xx[/ss])	10.10.10.1/8	Set Address
Link Status	Speed: 1000Mb/s, Full Duplex	Automatic <input type="button" value="Force Link"/>

**Subnets on this Interface**

Subnet	Local Address	Action
<input type="text"/>	<input type="text"/>	<input type="button" value="Add"/>
11.0.0.0/8	11.0.0.1	<input type="button" value="Delete"/>

If the unit is part of an HA configuration, the following screen will be displayed when clicking one of the interfaces.

Master 08:30:03 PM ■ ■ **Network Interface Management**

**Network Interface 0**

Interface Address (xxxxxxxxx[/ss])	10.10.10.1/8	Set Address
HA Shared IP address	10.10.10.7	Set Shared address
HA Partner IP address	10.10.10.3	Set Partner address
Use for HA checks	<input checked="" type="checkbox"/>	
Link Status	Speed: 1000Mb/s, Full Duplex	Automatic <input type="button" value="Force Link"/>

**Subnets on this Interface**

Subnet	Local Address	Action
<input type="text"/>	<input type="text"/>	<input type="button" value="Add"/>
11.0.0.0/8	11.0.0.1	<input type="button" value="Delete"/>

This screen tells the user:

- This is the Master machine of the pair (top left of the screen).
- This LoadMaster is up and the paired machine is down (green and red icons).
- The IP address of this LoadMaster.
- The HA shared IP address. This is the IP address used to configure the pair.

- The IP address of the paired machine.
- This interface is enabled for HA healthchecking
- The speed of the link is automatically detected.

## 7.2 Local DNS Configuration

**Set Hostname**

Current Hostname

Hostname Used for Diagnostic logging

**DNS Servers**

DNS NameServer (IP Address)	Action
<input type="text"/>	<input type="button" value="Add"/>
10.0.0.1	<input type="button" value="Delete"/>

**DNS Search Domains**

DNS Search Domains	Action
<input type="text"/>	<input type="button" value="Add"/>
10.0.0.1	<input type="button" value="Delete"/>

Max 3 dns servers and 6 search domains.

## 7.3 Route Management

This option permits the configuration of default and static routes. The Load Master requires a **default gateway** through which it can communicate with the Internet.

**The default gateway must be on the 10.0.0.0/8 network**

Default Gateway Address

Further routes can be added. These routes are static and the gateways must be on the same network as the Load Master. To segment traffic you can also leverage the Virtual Service level default gateway.

Destination	Gateway	Action
<input type="text"/>	<input type="text"/>	<input type="button" value="Add"/>

## 7.4 Access Control

### 7.4.1 Packet Filter Enabled

Using this toggle option the Packet filter can be activated/deactivated. If the filter is not activated, the Load Master acts as a simple IP-forwarder. When the filter is activated, only the Virtual Service addresses can be addressed.

Packet Filter

Rejection method  Drop  Reject

### 7.4.2 Reject/Drop blocked packets

When a connection request is received from a host, which is blocked using the ACL, the request is normally ignored (dropped). The Load Master may however be configured to send back an ICMP reject packet. For security reasons it is usually best to drop any blocked requests.

### 7.4.3 Access control Lists

The Load Master supports a “blacklist” Access Control List system. Any host or network entered into the Access Control List will be blocked from accessing any service provided by the Load Master.

Blacklist	
Blocked addresses	Operation
<input type="text"/>	<input type="button" value="Block Address(es)"/>

Whitelist	
Allowed addresses	Operation
<input type="text"/>	<input type="button" value="Allow Address(es)"/>

The Access Control List is only enabled when the Packet Filter is enabled. The whitelist allows a specific IP address or address range access. If the address or range is part of a larger range in the blacklist, the whitelist will take precedence for the specified addresses.

This option allows a user to add or delete a host or network IP address to the Access Control List. Only “dotted-quad” IP addresses are allowed. Using a network specifier specifies a network.

I.e. Specifying 192.168.200.0/24 will block all hosts on the 192.168.200 network.

## 7.5 System Administration

These options control the base level operation of LoadMaster. It is important to know that applying changes to these parameters in a HA pair must be done using the floating management IP. Many of these options will require a system reboot. When configuring these parameters only the active system in a pair is affected.

### 7.5.1 User Management

Change the appliance password. This is a local change only and does not affect the password of the partner appliance in a HA deployment.

Change Password		
Current Password	<input type="text"/>	
New Password	<input type="text"/>	
Re-enter New Password	<input type="text"/>	
<input type="button" value="Reset"/>		<input type="button" value="Set Password"/>

Other Users		
User	<input type="text"/>	
Password	<input type="text"/>	
Use RADIUS Server	<input type="checkbox"/>	
<input type="button" value="Add User"/>		

User	Permissions	Action
CMtest	Real Servers, Virtual Services, Rules, System Backup, 10.0.0.0/8	<input type="button" value="Modify"/> <input type="button" value="Delete"/> <input type="button" value="Password"/>

The User Management screen allows you to change a current Users password, add a new User and associated password or change the permissions for an existing User (see below).

Permissions for User CJMtest	
Real Servers	<input type="checkbox"/>
Virtual Services	<input type="checkbox"/>
Rules	<input type="checkbox"/>
System Backup	<input type="checkbox"/>
Certificate Creation	<input type="checkbox"/>
Intermediate Certificates	<input type="checkbox"/>
Certificate Backup	<input type="checkbox"/>
All Permissions	<input type="checkbox"/>
Allowed Network 1	None Assigned
Allowed Network 2	None Assigned

Buttons: Cancel, Reset, Set Permissions

In this screen you may set the level of User permissions insofar as what configuration changes they are allowed to perform. The primary User, bal, always has full permissions. Secondary Users may be restricted to certain functions and to certain networks.

### 7.5.2 Update License

Access Code information will be displayed on screen. This includes the activation date and the expiration date of the current license. To apply a new license enter the license code. A reboot may be required depending on which license you are applying.

Activation date: February 22 2011  
Licensed until: Unlimited

Please use the following Access Code to acquire a new license key from your KEMP representative for your LoadMaster.

Access Code: x7w3u-v4wbq-g1x88-9bx88 (Instance 232612)

License Key:

### 7.5.3 System Reboot

#### Reboot

Reboot the appliance.

#### Shutdown

Clicking the button attempts to power down the LoadMaster and if for some reason that fails, it will at a minimum halt the CPU.

#### Reset To Factory Defaults

Reset the configuration of the appliance with exception to the license information and usernames and passwords. This only applies to the active appliance in a HA pair.

Reboot

Shutdown

Reset To Factory Defaults

### 7.5.4 Update Software

Contact support to obtain the location of firmware patches and upgrades. Firmware download requires Internet access. Detailed patch information is available at <http://forums.kemptechnologies.com/viewforum.php?f=9>.

### **Update Machine**

Once you have downloaded the firmware you can browse to the file and upload the firmware directly into LoadMaster. The firmware will be unpacked and validated on LoadMaster. If the patch is validated successfully you will be asked to confirm the release information. To complete the update you will need to reboot the appliance, which can be deferred.

### **Restore Software**

If you have completed an update of LoadMasters firmware you can revert to the previous build.

## **7.5.5 Backup/Restore**

### **Create a Backup**

Generate a backup that contains the Virtual Service configuration and the local appliance information. License information and SSL Certificate information is not contained in the backup.

### **Restore Configuration**

When performing a restore (from a remote machine), the user may select what information should be restored:

The Virtual Service configuration

The LoadMaster Base Configuration

the LoadMaster configuration not including the Virtual Service configuration.

All the configuration information on the LoadMaster.

## **7.5.6 Date/Time**

You can manually configure the date and time of LoadMaster or leverage an NTP server.

### **NTP host(s)**

Specify the host which is to be used as the NTP server. NTP is a strongly preferred option for an HA cluster. For a single unit it is at the user discretion.



The time zone must always be set manually.

## 7.6 Logging Options

Logging of LoadMaster events can be both pushed and also pulled from the appliance. It is important to note that log files on LoadMaster are not historical, if the appliance reboots the logs are reset. It is important to keep a record of events generated on LoadMaster on a remote facility.

### 7.6.1 Log Files

Boot.msg File contains information during the initial starting of LoadMaster.

Warning Message File contains warnings during the operation of LoadMaster.

System Message File contains system events during the operation of LoadMaster, this included both operating system level and LoadMaster internal events.

Reset Logs will reset ALL log files.

Download all Log Files is used if you need to send logs to KEMP support as part of a support effort. Click this button, save the files to your PC and forward them to KEMP support.

Boot.msg File	View
Warning Message File	View
System Message File	View
Reset Logs	Reset
Save all Log Files	Download Log Files

Debug Options

### 7.6.2 Syslog Options

The LoadMaster can produce various warning and error messages using the syslog protocol. These messages are normally stored locally and may be displayed via the diagnostics menu point. It is also possible to configure the LoadMaster to transmit these error messages to a remote syslog server (menu point: extended->syslog).

Six different error message levels are defined and each message level may be sent to a different server. Notice messages are sent for information only; Emergency messages normally require immediate user action.




One point to note about syslog messages is they are cascading in an upwards direction. Thus, if a host is set to receive WARN messages, the message file will include message from all levels above WARN but none for levels below.



We recommend you do not set all six levels for the same host because multiple messages for the same error will be sent to the same host.

Emergency Host	<input type="text"/>
Critical Host	<input type="text"/>
Error Host	<input type="text"/>
Warn Host	<input type="text"/>
Notice Host	<input type="text"/>
Info Host	<input type="text"/>

 To enable a syslog process on a remote Linux server to receive syslog messages from the LoadMaster, the syslog must be started with the “-r” flag.

### 7.6.3 SNMP Options

With this menu, the SNMP configuration can be modified.

Enable/Disable SNMP metrics


This toggle option, enables or disables SNMP metrics. I.E. This option allows the LoadMaster to respond to SNMP requests.

**Note:** By default SNMP is disabled.

Enable SNMP	<input checked="" type="checkbox"/>
SNMP Clients	<input type="text"/>
Community String	public
Contact	<input type="text"/>
Location	<input type="text"/>
Enable SNMP Traps	<input type="checkbox"/>

Configure SNMP Clients

With this option, the user can specify from which SNMP management hosts the LoadMaster will respond to.

 If no client has been specified, the LoadMaster will respond to SNMP management requests from **any** host.

Configure SNMP Community String

This option allows the SNMP community string to be changed. The default value is “public”.

Configure SNMP Contact

This option allows the SNMP Contact string to be changed. For example, this could be e-mail address of the administrator of the LoadMaster.

Configure SNMP Location

This option allows the SNMP location string to be changed.

SNMP traps

When an important event happens to a LoadMaster a Virtual Service or to a Real Server, a trap is generated. These are sent to the SNMP trap sinks.

Enable/Disable SNMP Traps

This toggle option enables and disables the sending of SNMP traps.

**Note:** SNMP traps are disabled by default.

### Configure SNMP Trap Sink1

This option allows the user to specify a list of hosts to which a SNMPv1 trap will be sent when a trap is generated.

### Configure SNMP Trap Sink2

This option allows the user to specify a list of hosts to which a SNMPv2 trap will be sent when a trap is generated.

## 7.6.4 Email Options

This option permits the configuration of email alerting for LoadMaster events. Email notification can be delivered for six predefined informational levels. Each level can have a distinct email address and each level supports multiple email recipients. Email alerting depends on a mail server, support for both an open relay mail server and a secure mail server is provided. Testing email configuration can be done using the Web User Interface and navigating to System Configuration -> System Administration -> Logging Options -> Email Options

Sample Email Alert:



Oct 22 19:42:16 KEMP2 logger: This is a test from the Load Master

Enable Email Logging	<input checked="" type="checkbox"/>
SMTP Server	<input type="text"/> <input type="button" value="Set Server"/>
Server Authorization (Username)	<input type="text"/> <input type="button" value="Set"/>
Authorization Password	<input type="text"/> <input type="button" value="Set Password"/>
Local Domain	<input type="text"/> <input type="button" value="Set Domain"/>
Emergency Recipients	<input type="text"/>
Critical Recipients	<input type="text"/>
Error Recipients	<input type="text"/>
Warn Recipients	<input type="text"/>
Notice Recipients	<input type="text"/>
Info Recipients	<input type="text"/>
<input type="button" value="Reset"/> <input type="button" value="Change Email Recipients"/>	
<input type="button" value="Send Test Email to All Recipients"/>	

### Set SMTP Server

Enter the FQND or IP address of the mail server. If you are using FQDN please make sure to set the DNS Server.

### Set Authorized User

Enter the username if your mail server requires authorization for mail delivery. This is not required if you mail server does not require authorization.

### Set Authorized Users Password

Enter the password if your mail server requires authorization for mail delivery. This is not a required if you mail server does not require authorization.

### **Set Local Domain**

Enter the top-level domain if your mail server is part of a domain. This is not a required parameter.

### **Set Email Recipient**

Enter the email address that correspond with the level or notification desired. Multiple email addresses are supported by a space-separated list, such as:

INFO: [info@kemptechnologies.com](mailto:info@kemptechnologies.com) [sales@kemptechnologies.com](mailto:sales@kemptechnologies.com)

ERROR: [support@kemptechnologies.com](mailto:support@kemptechnologies.com)

## **7.7 Miscellaneous Options**

### **7.7.1 S-NAT Control**

This toggle option will either enable or disable the S-NAT functionality of the Load Master. When S-NAT is enabled, the Real Servers can access the Internet using the Load Master as a gateway. The Load Master will use “masquerading” so that connection requests from the Real Servers seem to originate on the Load Master. This means that the Real Servers can be on a private network and still have access to the Internet.

When S-NAT is disabled, the Load Master will not perform “masquerading” and so the Real Servers cannot access the Internet through the Load Master.



In Single-Armed configurations, S-NAT does not provide any extra functionality and we recommend it is turned off.

### **7.7.2 Remote Access**

Allow Remote SSH Access	<input checked="" type="checkbox"/>	Using: All Networks	Port: 22	<input type="button" value="Set Port"/>
		Disable SSH-V1 Prot <input checked="" type="checkbox"/>		
Allow Web Administrative Access	<input checked="" type="checkbox"/>	Using: eth0: 10.10.10.1	Port: 443	<input type="button" value="Set Port"/>
Administrative Default Gateway		<input type="button" value="Admin Default Gateway"/>		
Radius Server		<input type="button" value="Radius Server"/>	Shared Secret: <input type="text"/>	<input type="button" value="Set Secret"/>
Enable Hover Help	<input checked="" type="checkbox"/>			
Enforce Strict IP Routing	<input type="checkbox"/>			
Remote GEO LoadMaster Access		<input type="button" value="Set GEO LoadMaster access"/>		
GEO LoadMaster Port		22	<input type="button" value="Set GEO LoadMaster Port"/>	

#### **Allow Remote SSH Access**

You can limit the network from which clients can connect to the SSH administrative interface on LoadMaster.

#### **Allow Web Administrative Access**

This option allows you to assign the Interface address that will be hosting the Web User Interface access.

### **Administrative Default Gateway**

When administering the LoadMaster from a non-default interface, this option allows the User to specify a different default gateway for administrative traffic only.

### **RADIUS Server**

The address of the RADIUS server that is to be used to validate User access to the LoadMaster. To use RADIUS server you have to specify the shared secret.

### **Enable hover help**

Enables blue hover notes shown when the pointer is held over a field.

### **Remote GEO LoadMaster Access**

Set the addresses of the GEO LoadMasters that can retrieve service status information from this LoadMaster.

### **GEO LoadMaster Port**

The port over which GEO LoadMasters will use to communicate with this LoadMaster unit.

## **7.7.3 L7 Configuration**

L7 Transparency	Non Transparent
Allow connection scaling over 64K Connections	No
L7 Connection Drain Time (secs)	300 <input type="button" value="Set Time"/> (Valid values:60 - 86400)
Additional L7 Header	X-ClientSide
Add Port to Active Cookie	No
L7 Connection Timeout (secs)	0 <input type="button" value="Set Time"/> (Valid values:0, 60-86400)
Always Check Persist	No
Assume Expect-100	No
Conform to RFC	Yes

### **L7 Transparency**

This is a global configuration for all Layer 7 Virtual Services.

### **Allow Connection Scaling over 64K Connections**

Under very high load situations, Port Exhaustion can occur. Enabling this option will allow the setting of Alternate Source Addresses which can be used to expand the number of local ports available.

### **L7 Connection Drain Time (secs)**

The number of seconds a persistence entry is permitted to override the disablement of a Real Server. Once a Real Server has been disabled, existing clients with a valid persistence to this server will be permitted to return. Once over the time interval they will be scheduled to a new Real Server via the scheduling method.

### **Additional L7 Header**

This enables Layer 7 header injection for HTTP/HTTPS Virtual Services. Header injection can be set to X-ClientSide (KEMP LoadMaster specific) or X-Forwarded-For, or None. Refer to the Transparency Guide for an explanation of transparency and the value of header injection.

### ***Add Port to Super HTTP***

When this option is enabled, the LoadMaster will incorporate the client's source port number in the Super HTTP value issued. For Active Super HTTP persistence, the Active Super HTTP (or Active-Super HTTP -Source) persistence mode must still be enabled on a Virtual Service. This parameter can be of value when client traffic arrives at the LoadMaster via NATting proxy servers or firewalls. Without port inclusion, all client traffic from a given IP address will be directed to the same Real Server, with a potential for "lumpy" load balancing.

### ***L7 Connection Timeout***

The number of seconds that all Layer 7 Virtual Services can have no activity, the connection is closed after the timeout is reached.

### ***Always Check Persist***

Override the default optimized behavior to only check persistence on initial TCP/IP connection.

### ***Assume Expect-100***

By default the L7 module will only wait for 100-Continue replies if it sees an Expect-100 header. Enabling this option will always wait for 100-Continue messages. Contact KEMP support prior to changing this value.

### ***Conform to RFC***

This option addresses parsing the header of an HTTP request in conformance with RFC 1738

The request consists of 3 parts: GET /pathname HTTP/1.1 and when "conform" is on, the LoadMaster scans through the pathname until it finds a space. It then presumes that the next thing is HTTP/1.x. If the pathname contains spaces and the browser is conformant to the RFC, the pathname will have the spaces escaped to "%20" so the scan for a space still functions correctly.

However, on some broken browsers, spaces are not escaped and the wrong pathname is processed. And since the system can't find the HTTP/1.x, the LM will reject the request.

Turning off this feature, forces the LM to assume that the pathname extends to the last space on the line. It is then assumed that what follows is HTTP/1.x. So making pathnames with spaces in them useable – however, it is non-conformant to the RFC 1738.

## ***7.7.4 AFE Configuration***

### ***Maximum Cache Size***

How much memory can be utilized by the cache in Mbytes.

### ***Cache Virtual Hosts***

When not enabled the cache presumes there is only one virtual host supported on the Real Server. Enabling this option allows the cache to support multiple virtual hosts which have different content.

**Cache Configuration**

Maximum Cache Size	100 <input type="button" value="Set Size"/> (Valid values:1 - 203)
Cache Virtual Hosts	No ▾
File extensions that should not be cached: . <i>aspx .jsp .php .html</i>	<input type="text"/> <input type="button" value="Add"/> No Entry ▾ <input type="button" value="Delete"/>

**Compression Options**

File extensions that should not be compressed: . <i>asf .gif .gz .jpeg .jpg .mov .mp3 .mp4 .mpe .mpeg .mpg .pdf .png .swf .tgz .wav .wma .wmv .z .zip</i>	<input type="text"/> <input type="button" value="Add"/> No Entry ▾ <input type="button" value="Delete"/>
--	---

**Intrusion Detection Options**

Detection Rules	<input type="button" value="Browse..."/>	<input type="button" value="Install new Rules"/>
Detection level	Default - Only Critical problems are rejected ▾	

**File Extensions Not to Cache**

A list of files types that should not be cached.

**File Extensions Not to Compress**

A list of file types that should not be compressed.

**Intrusion Detection**

Supports four levels of what to do when problems are encountered.

<b>Low</b>	–	only	logging	with	no	rejection
<b>Default</b>	–	only	critical	problems	problems	rejected
<b>High</b>	–	Serious	and	critical	problems	rejected
<b>Paranoid</b>	– All detected problems rejected					

**7.7.5 Network Options**

Enable Non-Local Real Servers	No ▾
Enable Alternate GW support	No ▾
Enable TCP Timestamps	No ▾
Enable TCP Keepalives	No ▾
Enable Reset on Close	No ▾
Subnet Originating Requests	No ▾

**Enable Non-Local Real Servers**

Allow non-local Real Servers to be assigned to Virtual Services.

**Enable Alternate GW support**

Provides the ability to move the default gateway to a different interface.

**Enable TCP Timestamps**

The LoadMaster can include a timestamp in the SYN when connecting to Real Servers.



Enable this only upon request from KEMP support.

### ***Enable TCP Keepalives***

By default the TCP keepalives are enabled which improves the reliability of TCP connections that are long lived (SSH sessions). Keepalives are not usually required for normal HTTP/HTTPS services.



The keepalive messages are sent from the LoadMaster to the Real Server and to the Client. Therefore, if the Client is on a mobile network, there may be an issue with additional data traffic.

### ***Enable Reset on Close***

When enabled the LoadMaster will close its connection with the Real Servers by using RESET instead of the normal close handshake. This only makes a difference under highloads of many connections.

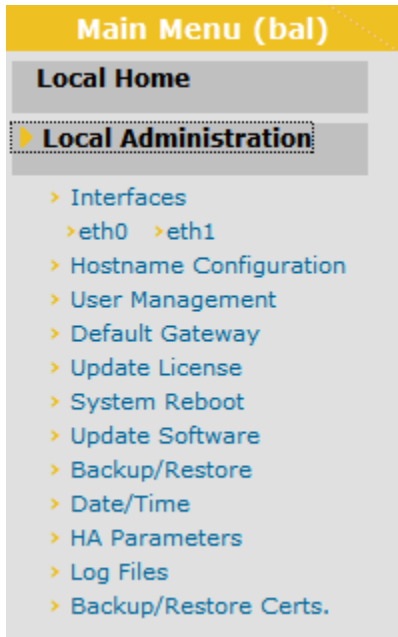
### ***Subnet Origination Requests***

When transparency is turned off for a Virtual Service, the source IP address of connections to the Real Servers is the Virtual Service. When enabled, and subnets are being used, the source IP address will be the subnet local address of the LoadMaster. If the Real Server is on a subnet, then the subnet address of the LoadMaster will be used.

### 7.7.6 HA Parameters

The role of the appliance can be changed by setting the HA Mode. Changing the HA Mode will require a reboot, once LoadMaster has rebooted HA Parameter will appear provided the role is not "Non HA Mode". HA will NOT work if both machines are specified the same.





When logged into the HA pair, use the shared IP address to view and set full functionality to the pair. If you log into the direct IP address of either one of the devices the menu options are dramatically reduced (see menu below). Logging into one of the pair is usually reserved for maintenance



HA Mode	HA (First) Mode
HA version	Upgraded (carp)
HA Timeout	9 Seconds
HA Initial Wait Time	0 <input type="button" value="Set Delay"/> ( Valid Values: 0, 10-180)
HA Virtual ID	1 <input type="button" value="Set Virtual ID"/> ( Valid Values: 1-255)
Switch to Preferred Server	No Preferred Host
HA Update Interface	eth0:
Inter HA L4 TCP Connection Updates	<input type="checkbox"/>
Inter HA L7 Persistency Updates	<input type="checkbox"/>

### HA Status

At the top of the screen, next to the date and time, icons are shown to denote the status of the LoadMaster units in the cluster. There will be an icon for each unit in the cluster. The four possible icons are:

- |                   |   |   |
|-------------------|---|---|
| <b>Green</b>      |  | The unit is online and operational and the HA units are correctly paired.   |
| <b>Red/Yellow</b> |  | The unit is not ready to take over. It may be offline or incorrectly paired.  |
| <b>Grey</b>       |  | The unit is pacified, i.e. it has rebooted more than 3 times in 5 minutes. In this state you can only access the machine via the machine WUI (not the shared WUI), and, it is not participating in any HA activity, i.e. no changes from the master will be received and it will not take over if the master fails. |
| <b>Blue</b>       |  | BOTH machines are active, i.e. both are set to master, and something has gone seriously wrong. <b>CALL KEMP support.</b>  |

In HA mode each LoadMaster will have its own IP address used only for diagnostic purposes directly on the unit. The HA pair have a shared IP address over which the WUI is used to configure and manage the pair as a single entity.

### **HA Mode**

If using a single LoadMaster, select Non-HA Mode. When setting up HA mode, on LoadMaster must be set to HA (First) and the other HA (Second). If they are both set to the same, HA will not operate.



KEMP supplies a license that is HA enabled for each HA unit and specifies first or second unit. Therefore it is not recommended that you change this option until you have discussed the issue with KEMP.

### **HA Version**

By default the system uses a version of VRRP (CARP - Common Address Redundancy Protocol) to check the status of the partner. The systems can also support the legacy heartbeat program. Changes to this option requires both machines to be rebooted for the change to take effect.

### **HA Timeout**

The time that the Master machine must be unavailable before a switchover occurs. With this option, the time it takes an HA cluster to detect a failure can be adjusted from 3 seconds to 15 seconds in 3 second increments. The default value is 9 seconds. A lower value will detect failures sooner, whereas a higher value gives better protection against a DOS attack.

### **HA Initial Wait Time**

How long after the initial boot of a LoadMaster, before the machine decides that it should become active. If the partner machine is running, then this value is ignored. This value can be changed to mitigate the time taken for some intelligent switches to detect that the LoadMaster has started and to bring up the link

### **HA Virtual ID**

When using multiple HA LoadMasters on the same network, this value identifies each cluster so that there are no potential unwanted interactions.

### **Switch to Preferred Server**

By default, neither partner in a HA cluster has priority. So that when a machine restarts after a switchover, the machine becomes slave. Specifying a preferred host means that when this machine restarts, it will always become master and the partner will revert to slave mode.

### ***HA Update Interface***

The interface used to synchronize the HA information within an HA cluster.

### ***Inter HA L4 TCP Connection Updates***

When using L4 services, enabling updates will allow L4 connections to be maintained across a HA switchover. This option is ignored for L7 services.

### ***Inter HA L7 Persistency Updates***

When using L7 services, enabling this option will allow persistence information to be shared between the HA partners. If a HA failover occurs, the persistence information will not be lost. Enabling this option can have a significant performance impact.

## 4. Appendix

### A. Persistence Table

Persistence methods supported by each Exchange 2010 CAS Service

	Workload	Preferred Session Persistence Method
HTTP-Based Workloads	Outlook Web App (OWA)	1. Source IP 2. Super HTTP
	Control Panel (ECP)	1. Source IP 2. Super HTTP
	ActiveSync (EAS)	1. Source IP 2. Authorization header
	Web Services (EWS)	1. Super HTTP 2. SSL ID
	Outlook Anywhere (OA)	1. Source IP 2. No affinity/persistence
	Autodiscover Service (AS)	No affinity/persistence
TCP Socket Oriented Workloads	RPC Client Access Service (RPC CA)	1. Source IP
	Address Book (EAB)	1. Source IP
	RPC Endpoint Mapper	1. Source IP
	Post Office Protocol version 3 (POP3)	No affinity/persistence
	Internet Message Access Protocol version 4 (IMAP4)	No affinity/persistence
	Simple Mail Transfer Protocol (SMTP)	No affinity/persistence

## B. Connection Scaling For Large Scale Deployments

Execution of this procedure is optional and should be used only in cases where you expect your network traffic to be greater than 64,000 server connections at any one particular time.

You must disable L7 Transparency in order to use connection scaling.

To use connection scaling, click System Configuration.

Click Miscellaneous Options.

Click L7 Configuration.

Use the Allow connection scaling over 64K Connections drop down list and select Yes.

Allow connection scaling over 64K Connections	Yes ▾
---	-------

Click Virtual Services.

Click View/Modify Services.

Click the **Modify** button of the appropriate (presumably just created) Virtual IP Address.

In the **Advanced Properties** panel, input a list of **Alternate Source Addresses**. Multiple IPV4 addresses must be separated with a space, each must be unallocated and allow 64K connections.

Click the Set Alternate Addresses button.

Return to the next step of the configuration procedure you were following prior to executing this procedure.

## C. Configuration Table

The table indicates which values to use when configuring your LoadMaster for Exchange 2010.

Client or Service	Real Server Check Parameters	Port/Protocol	Scheduling Method	SSL Acceleration
AutoD	HTTP Protocol URL: "/owa"	80/TCP, 443/TCP (SSL)	round robin	Enabled
EAS	HTTP Protocol URL: "/microsoft-server-activesync"	80/TCP, 443/TCP (SSL)	round robin	Enabled
ECP	HTTP Protocol URL: "/ecp"	80/TCP, 443/TCP (SSL)	round robin	Enabled
EWS	HTTP Protocol URL: "/ews/exchange.asmx"	80/TCP, 443/TCP (SSL)	round robin	Enabled
OA	HTTP Protocol URL: "/rpc/rpcproxy.dll"	80/TCP, 443/TCP (SSL)	round robin	Enabled
OWA	HTTP Protocol URL: "/owa"	80/TCP, 443/TCP (SSL)	round robin	Enabled
IMAP4	Mailbox (IMAP) Protocol	143/TCP (TLS)	round robin	Disabled
IMAP4-S	TCP Protocol	993/TCP (SSL)	round robin	Enabled
POP3	Mailbox (POP3) Protocol	110/TCP (TLS)	round robin	Disabled
POP3-S	TCP Protocol	995/TCP (SSL)	round robin	Enabled
SMTP	Mail (SMTP) Protocol	25/TCP	round robin	Disabled
SMTP-S	TCP Protocol	587/TCP (SSL)	round robin	Enabled
MAPI (RPC)	TCP Connection Only (port 135)	* /TCP, TCP 1024-65535	round robin	Disabled



The high number port is for use with SSL, however, Health Checking is unencrypted. In this configuration regular TCP Health Checking should be used.

## 5. Glossary

The following table lists the meanings of acronyms used throughout this manual.

Acronym	Meaning
AD LDS	Active Directory Lightweight Directory Services
AutoD	AutoDiscover
CAS	Client Access Server
DNS	Domain Name System
EAS	ActiveSync
ECP	Control Panel
EWS	Web Services
FQDN	Fully Qualified Domain Name
IMAP4	Internet Message Access Protocol
MAPI	Messaging Application Program Interface
MX	Mail
NAT	Network Address Translation
OA	Outlook Anywhere. Previously known as RPC over HTTP.
OAB	Offline Address Book
OWA	Outlook Web App. Previously known as Outlook Web Access.
PFX	Personal Information File
POP3	Post Office Protocol
RPC	RPC Client Access Service. A windows proxy service component.
SLB	Server Load Balancer
SMTP	Simple Mail Transfer Protocol
SSL	Secure Socket Layer
TCP	Transmission Control Protocol
VIP	Virtual IP
WNLB	Windows Network Server load balancing

## 6. Index

	<b><u>A</u></b>		<b><u>M</u></b>
AD LDS, 53		MAPI, 7, 12, 52, 53	
AFE, 44			<b><u>N</u></b>
	<b><u>B</u></b>		
Backup, 38		NAT, 16, 24, 42, 53	
	<b><u>C</u></b>		<b><u>O</u></b>
CAS, 5, 8, 10, 53		OA, 5, 8, 11, 50, 52, 53	
Certificate, 38		OAB, 11, 53	
Content Rule, 28		OWA, 5, 8, 11, 50, 52, 53	
Content Switching, 22, 24			<b><u>P</u></b>
Cookie, 19, 44		Persistence, 19, 20, 23	
	<b><u>D</u></b>	POP3, 5, 8, 12, 50, 52, 53	
DNS, 53			<b><u>R</u></b>
	<b><u>E</u></b>		
EAS, 5, 8, 11, 12, 50, 52, 53		Real Server, 16, 18, 22, 24, 25, 30, 43, 44	
ECP, 11, 50, 53		Restore, 38	
EWS, 11, 50, 53		RPC, 5, 7, 8, 11, 12, 50, 52, 53	
	<b><u>F</u></b>		<b><u>S</u></b>
FQDN, 8, 53		SMTP, 5, 6, 8, 16, 41, 50, 52, 53	
	<b><u>H</u></b>	S-NAT, 42	
HA, 36, 37, 47, 48, 49		SNMP, 40, 41	
	<b><u>I</u></b>	SSL, 5, 8, 9, 18, 20, 21, 23, 38, 50, 52, 53	
ICMP, 18, 24, 36			<b><u>T</u></b>
IMAP4, 5, 12, 50, 52, 53		TCP, 10, 50, 52, 53	
	<b><u>L</u></b>		<b><u>V</u></b>
L7, 16, 43, 44, 49			
L7 Transparency, 16, 43		VIP, 8, 53	
		Virtual Services, 15, 16, 23, 30, 44	

## 7. Document History

Date	Change	Reason for Change	Resp.
Apr 2011	Updated various configuration instructions.	Periodic revision	CJM
Aug 2011	Updated features	Updated to latest GA	CJM