



# LoadMaster Deployment Guide

For

# Microsoft Exchange 2010

Updated: November 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**

<i>Table of Contents</i> .....	3
1. About KEMP Technologies .....	4
Load Balancing Microsoft Server 2010.....	4
About This Manual .....	5
Prerequisites.....	5
2. Exchange 2010 Overview .....	6
Understanding Server Load Balancing .....	6
Advantages to using a KEMP LoadMaster .....	7
Optimizing the KEMP LoadMaster for Microsoft Exchange 2010.....	7
SSL Acceleration (SSL Offloading).....	8
L7 Transparency .....	9
Persistence .....	9
Idle Connection Timeout .....	9
Port Configuration .....	9
Connection Scaling .....	10
Header Rewriting .....	10
Preconfigured Virtual Services .....	10
RPC Client Access Service .....	10
Hub-Edge-SMTP .....	10
Enforce Secure Access .....	10
All HTTPS Services.....	10
3. Load Balancing Client Access Server Services .....	11
Configuring KEMP LoadMaster with a Consolidated Virtual Service for HTTPS-based Exchange 2010 Clients and Services .....	12
Configuring a Virtual Service for HTTPS-based services (with SSL Offload) .....	12
Configuring a Virtual Service for HTTPS-based services (w/out SSL Offload) .....	14
Configuring KEMP LoadMaster for Outlook MAPI .....	15
Configuring KEMP LoadMaster with unique Virtual Services.....	15
Outlook Web App (OWA) .....	16
Control Panel (ECP).....	18
ActiveSync (EAS).....	19
Outlook Anywhere (OA) .....	21
Web Services (EWS).....	23
Autodiscover Service (AS) .....	25
Internet Message Access Protocol (IMAP4) .....	26
Post Office Protocol (POP3).....	29
4. Edge Transport Servers - Configuring KEMP LoadMaster for SMTP.....	30
5. Appendix.....	33
Persistence Methods Supported by each Exchange 2010 CAS Service.....	33
Connection Scaling For Large Scale Deployments.....	34
Configuration Table.....	35
6. Glossary.....	36
7. Index.....	37
8. Document History.....	38

## 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 combines versatility with ease-of-use to speed deployment of the complete portfolio of advanced messaging applications and protocols used by 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 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 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 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 (U.S.A.) or +1 353 61 260101 (Europe)

## About This Manual

This manual addresses how to deploy and configure a LoadMaster appliance with Microsoft 2010. Specifically, configuration information applies to Outlook Web App (OWA), Control Panel (ECP), ActiveSync (EAS), Outlook Anywhere (OA), Internet Message Access Protocol (IMAP), Post Office Protocol (POP), RPC Client Access (RPC CA), Address Book service (EAB), AutoDiscover (AS), Offline Address Book (OAB), Web Services (EWS) and Simple Message Transfer Protocol (SMTP).

Kemps' LoadMaster family of products is available in various models to support networks of different throughput requirements. Information in this manual applies to all LoadMaster models.

Images used in this manual are samples to help you determine if you are "in the right place" when actually performing the configuration.

Certain procedures contain instructions that refer to a Website. If you are configuring your LoadMaster at the same time you wish/need to access a Website then you should do so in a new and different browser session (i.e. do not use your web browser to access/configure the LoadMaster 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).

## Prerequisites

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

You should have reviewed the LoadMaster Quick Start Installation documentation and the LoadMaster Configuration Guide. Documentation is 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 on the same network as the Servers.

Established access to the LoadMaster Web User Interface.

*Recommended:* changed the default gateway on the Real Servers to point to the LoadMaster. 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.

### 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.

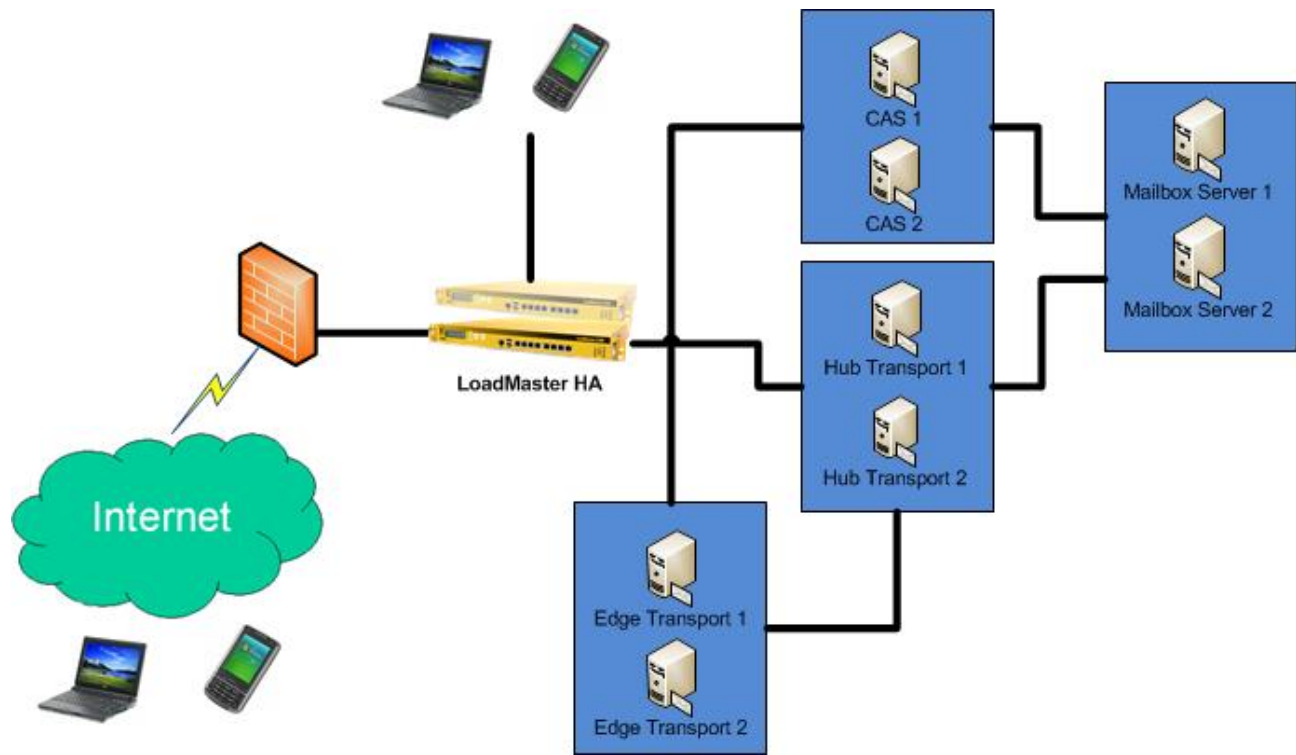
Server load balancing reduces the impact of a single Client Access Server failure within one of your Active Directory sites and ensures that the load on your Servers is evenly distributed. Architectural changes with respect to earlier versions of make server load balancing even more important than in 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/fff625247.aspx> .

## Advantages to using a KEMP LoadMaster

KEMP LoadMaster 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.



When a KEMP LoadMaster based CAS array has been configured, all servers in the array can be represented by a single VIP address and an FQDN (Fully Qualified Domain Name). 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.

## Optimizing the KEMP LoadMaster for Microsoft Exchange 2010

Your KEMP LoadMaster has features and capabilities in addition to those described in this manual, however, these features and capabilities in particular can be used to optimize the configuration of LoadMaster to work best with your Exchange 2010 server load balancing requirements.

## SSL Acceleration (SSL Offloading)

The KEMP LoadMaster offers SSL acceleration (also referred to as “SSL offloading”) for Virtual Services. With SSL acceleration, the SSL session is terminated at the LoadMaster . Some of the benefits to using SSL acceleration are that the LoadMaster migrates the SSL workload from the Real Servers (which can be hardware accelerated by LoadMaster ), can perform Layer 7 processing (such as 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 and sent to the Real Servers un-encrypted. In some security situations, it may be necessary to encrypt the connection between the LoadMaster and Real Servers. This can be achieved with reverse SSL. Review the LoadMaster manual to configure a reverse SSL deployment.

With reverse SSL, the SSL session is first terminated at the LoadMaster . 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 and the Real Server.

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

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

With software SSL, the LoadMaster 's general processor handles encryption/decryption tasks. These tasks are shared with other tasks that the LoadMaster 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 may degrade overall performance of the LoadMaster .

With hardware SSL, the LoadMaster has a separate specialized processor, which handles all SSL functions. No matter the level of SSL connections, the LoadMaster '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 , there are two types of SSL certificates: self-signed certificates generated by the LoadMaster or the administrator and certificates that are signed by a trusted CA (Certificate Authority) such as Digicert, Verisign or Thawte. In addition, with LoadMaster 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 , 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 .

## L7 Transparency

Newly created Virtual Services on a LoadMaster are set Transparent on a LoadMaster by default. In Transparent mode, the LoadMaster 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. 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. Typically, this is achieved by making the LoadMaster 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 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 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

If there is no traffic for the period of time specified the connection is timed out and disconnected. The global default is 660 seconds (11 minutes). This value should be adjusted per service type.

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 you should not set these timeout values 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.

 The value in the field may show as a zero, which means the global default is the value used by the LoadMaster. The global value is set in the System Configuration; Miscellaneous Options; L7 Configuration; L7 Connection Timeout.

## Port Configuration

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 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 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 offers HTTP header insertions, deletions, and modifications. Our header rewriting feature can be useful with respect to the URL users must input or remember.

## Preconfigured Virtual Services

The LoadMaster *Exchange* appliance and the Virtual LoadMaster Exchange products both come preconfigured with four basic services that will allow most users to start using the LoadMaster right away without the need to setup additional VS's. The four preconfigured services are:

### RPC Client Access Service

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

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

### Hub-Edge-SMTP

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


### Enforce Secure Access

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

### All HTTPS Services

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

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

 These VS's are treated as any other VS and may be modified or deleted, as required. For more information see the LoadMaster *Exchange* Configuration Guide.

### 3. Load Balancing Client Access Server Services

This section provides step by step instructions on how you configure the KEMP LoadMaster to load balance the various services of Microsoft Exchange 2010.

Each service handled by the Client Access Server (CAS) 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.

## Configuring KEMP LoadMaster with a Consolidated Virtual Service for HTTPS-based Exchange 2010 Clients and Services

For most configurations KEMP recommends creating a single Virtual Service for all HTTPS-based Exchange 2010 clients and services. That is a Virtual Services used by Outlook Web App (OWA), Control Panel (ECP), Outlook Anywhere (OA), Offline Address Book (OAB), ActiveSync (EAS), Web Services (EWS) and the Autodiscover service.

Using a single Virtual Service keeps the load balancer configuration simple and lets you have a single FQDN and associated SSL certificate for all Exchange 2010 client access methods and services.

You may use the same FQDN and SSL certificate for IMAP4 and POP3 access, even though they are on different Virtual Services, since they don't use port 443 like the above-mentioned client access methods and services.

## Configuring a Virtual Service for HTTPS-based services (with SSL Offload)


### Prerequisites

When you choose to offload SSL, you should follow the recommendations set by Microsoft. KEMP Technologies understands these recommendations to be **(a)** enable SSL Offloading for (as per instructions) [http://technet.microsoft.com/en-us/library/bb885060\(EXCHG.80\).aspx](http://technet.microsoft.com/en-us/library/bb885060(EXCHG.80).aspx) and **(b)** disable "Require SSL" on IIS [http://technet.microsoft.com/en-us/library/cc732341\(WS.10\).aspx](http://technet.microsoft.com/en-us/library/cc732341(WS.10).aspx).

1. Connect and log in to your LoadMaster .
2. Create a Virtual Service. Click **Virtual Services** and then click **Add New**.

**Please Specify the Parameters for the Virtual Service.**

Virtual Address	<input type="text"/>
Port	443
Protocol	tcp

3. Enter the **Virtual Address** using the format `###.###.###.###`.
4. Enter 443 as the **Port**.
5. Select **tcp** as the **Protocol**.
  -  *The combination of Virtual Address, Port and Protocol must be unique within LoadMaster.*
6. Click **Add this Virtual Service**.
7. Select the **L7 Transparency** check box.
8. Enter a **Service Nickname**. This is for display purposes only. For example, "2010 HTTPS". Click **Set Nickname**.
9. For **Persistence Options**, select **Super HTTP** as the **Mode**. Use the **Timeout** drop down list to select **1 Hours**.
10. Select **round robin** as the **Scheduling Method**.
11. Offload SSL by selecting the **Enabled** check box for **SSL Acceleration**. By default, a self-signed certificate is used; therefore, click **OK** when a message displays indicating that there is no SSL certificate currently available for your Virtual Service and that a temporary one will be used until a valid certificate is installed.
12. For **Rewrite Rules**, use the drop down list and select **HTTPS**.
13. Optional: If you have not already done so, export the appropriate certificate and key from Exchange 2010 using the Microsoft export information found at <http://technet.microsoft.com/en-us/library/bb310778.aspx>. You want to make sure to export the certificate and private key as a Personal Information File (PFX). You can also obtain an SSL certificate that you desire from any certificate authority. When prompted by a third party certificate authority to specify a server type, indicate "Apache". The format of Apache server type certificates is recognized by LoadMaster .
14. Optional: If you have not already done so, import the appropriate PFX certificate and key file into LoadMaster . To import, click the **Add New** button of the **Certificates** field. Click the **Browse** button, locate and open the PFX file. Next, click the **Submit** button.
15. For Real Server Check Parameters select HTTP Protocol. You will need to input a URL in the **URL: edit window** and click **Set URL**. The content of this field should be reflected based on what service you want checked. Review the Configuration Table in Appendix 5. As an example, if you were configuring Outlook Anywhere (OA), you would input `/rpc/rpcproxy.dll`.
16. Input `"FRONT-END-HTTP": "ON"` into the **Add Header to Request** edit window. Click **Set Header**. *Legacy header injection carried forward, not required as per Microsoft.*
17. Add Real Servers. Click **Add New...**


- For each CAS, input its IP as the **Real Server Address** on **Port 80**. Click **Add This Real Server**.

**Please Specify the Parameters for the Real Server**

Real Server Address	<input type="text"/>
Port	80
Forwarding method	nat
Weight	1000

- Click **OK** in response to the confirmation that the Real Server was added.
- You have now completed your configuration of LoadMaster for Exchange 2010. If you wish to view, modify, or delete any Real Servers that have been added, click **View/Modify Services**.

### Configuring a Virtual Service for HTTPS-based services (w/out SSL Offload)

- Connect and log in to your LoadMaster .
- Create a Virtual Service. Click **Virtual Services** and then click **Add New**.
- Enter the **Virtual Address** using the format **###.###.###.###**.
- Enter 443 as the **Port**.
- Select **tcp** as the **Protocol**.
  -  *The combination of Virtual Address, Port and Protocol must be unique within LoadMaster.*
- Click **Add this Virtual Service**.
- Select the **Force L7** check box.
- Select the **L7 Transparency** check box.
- Enter a **Service Nickname**. This is for display purposes only. For example, "OA-EAS-EWS-WOSSL". Click **Set Nickname**.
- For **Persistence Options**, select **Source IP Address** as the **Mode**. Use the **Timeout** drop down list to select **1 Hours** and the **Netmask** drop down list to select **/32**.
- Select **round robin** as the **Scheduling Method**.
- For **Real Server Check Parameters** select **HTTPS Protocol**.
- Add Real Servers. Click **Add New...**
- For each CAS, input its IP address as the **Real Server Address** on **Port 443**. Click **Add This Real Server**.
- Click **OK** in response to the confirmation that the Real Server was added.
- You have now completed your configuration of LoadMaster for Exchange 2010. If you wish to view, modify, or delete any Real Servers that have been added, click **View/Modify Services**.

## Configuring KEMP LoadMaster for Outlook MAPI



The following steps are required in order to create the Virtual Service for Outlook MAPI connectivity:

### Creating the Virtual Service for the RPC CA (MAPI) & Address Book Service

1. Create a Virtual Service. Click **Virtual Services** and then click **Add New**.
2. Input the **Virtual Address** using the format `###.###.###.###`.
3. Input "\*" (asterisk only, not the quotes) as the **Port**. *If you wish to configure your Exchange 2010 environment to utilize static RPC ports as opposed to the dynamic port range realized by inputting the asterisk, you should first configure your Exchange 2010 Server by following the instructions at <http://social.technet.microsoft.com/wiki/contents/articles/configuring-static-rpc-ports-on-an-exchange-2010-client-access-server.aspx>. You can then input into LoadMaster a specific port number for each Virtual Service.*



**Do not change the Wildcard service to L4. Doing so will cause inoperability.**

4. Select **tcp** as the **Protocol**.
  -  *The combination of Virtual Address, Port and Protocol must be unique within LoadMaster.*
5. Click **Add this Virtual Service**.
6. Ensure the **Force L7** checkbox is selected.
7. Select the **L7 Transparency** check box.
8. Enter a **Service Nickname**. This is for display purposes only. For example, "MAPI". Click **Set Nickname**.
9. For **Persistence Options**, select **Source IP Address** as the **Mode**. Use the **Timeout** drop down list to select **1 Hours** and the **Netmask** drop down list to select **255.255.255.255**.
10. Select **round robin** as the **Scheduling Method**.
11. Enter 86,400 as the **Idle Connection Timeout** and click **Set Idle Timeout**.
  -  *This will provide an idle timeout of 24 hours and prevent Outlook Users having to re-authenticate during the working day.*
12. For **Real Server Check Parameters** select **TCP Connection Only** and specify port 135.
13. Add Real Servers. Click **Add New...**
14. Enter the same () **Real Server Address**. Click **Add This Real Server**.
15. Click **OK** in response to the confirmation that the Real Server was added.
16. You have now completed your configuration of LoadMaster for Exchange 2010. If you wish to view, modify, or delete any Real Servers that have been added, click **View/Modify Services**.

### Configuring KEMP LoadMaster with unique Virtual Services

By maintaining a unique Virtual Service for each CAS service, you can manage each independently from one another. For example, you may wish to have different pool membership,

server load balancing methods, or custom monitors for OWA and OA. If those services are each associated with a different Virtual Service, micro-management becomes easier.

### Important

When using a unique Virtual Service for each CAS service, you cannot share the same FQDN and port among the services. So for HTTPS-based services, you should use unique FQDNs for each CAS service and Virtual Service. This is a general limitation when load balancing services using layer 7.


In the following we show the steps necessary for creating a Virtual Service for each of the available Client Access services in Exchange 2010.

## Outlook Web App (OWA)

### Configuring a Virtual Service for OWA (with SSL Offload)


When you choose to offload SSL for OWA, you should follow the recommendations set by Microsoft. KEMP Technologies understands these recommendations to be (a) enable SSL Offloading for (as per instructions)

[http://technet.microsoft.com/en-us/library/bb885060\(EXCHG.80\).aspx](http://technet.microsoft.com/en-us/library/bb885060(EXCHG.80).aspx) and (b) disable "Require SSL" on IIS [http://technet.microsoft.com/en-us/library/cc732341\(WS.10\).aspx](http://technet.microsoft.com/en-us/library/cc732341(WS.10).aspx).

1. Connect and log in to your LoadMaster .
2. Create a Virtual Service. Click Virtual Services and then click Add New.
3. Enter the Virtual Address using the format ###.###.###.###.
4. Enter 443 as the Port.
5. Select tcp as the Protocol.  
 The combination of Virtual Address, Port and Protocol must be unique within LoadMaster.
6. Click Add this Virtual Service.
7. Select the **L7 Transparency** check box.
8. Enter a Service Nickname. This is for display purposes only. For example, " 2010 OWA". Click Set Nickname.
9. For Persistence Options, select a Layer 7 organic persistence method as the Mode. Use the Timeout drop down list to select 1 Hours and the Netmask drop down list to select /32.
10. Select round robin as the Scheduling Method.
11. Input 900 as the Idle Connection Timeout and click Set Idle Timeout.
12. Offload SSL by selecting the Enabled check box for SSL Acceleration. By default, a self-signed certificate is used; therefore, click OK when a message displays indicating that there is no SSL certificate currently available for your Virtual Service and that a temporary one will be used until a valid certificate is installed.
13. Optional: If you have not already done so, export the appropriate certificate and key from Exchange 2010 using the Microsoft export information found at <http://technet.microsoft.com/en-us/library/bb310778.aspx>. You want to make sure to export the certificate and private key as a Personal Information File (PFX). You can also obtain an SSL certificate that you desire from any certificate authority. When prompted by a third party certificate authority to specify a server type, indicate "Apache". The format of Apache server type certificates is recognized by LoadMaster .

14. Optional: If you have not already done so, import the appropriate PFX certificate and key file into LoadMaster . To import, click the Add New button of the Certificates field. Click the Browse button, locate and open the PFX file. Next, click the Submit button.
15. For Real Server Check Parameters select HTTP Protocol. Input “/owa” in the URL: edit window and click Set URL.
16. Input “FRONT-END-HTTP”:“ON” into the Add Header to Request edit window. Click Set Header. Legacy header injection carried forward, not required as per Microsoft.
17. Add a port 80 redirector Virtual Service.
18. Add Real Servers. Click Add New...
19. For each CAS, input its IP as the Real Server Address on Port 80. Click Add This Real Server.
20. Click OK in response to the confirmation that the Real Server was added.
21. You have now completed your configuration of LoadMaster for Exchange 2010. If you wish to view, modify, or delete any Real Servers that have been added, click **View/Modify Services**.

### Configuring a Virtual Service for OWA (without SSL Offload)


1. Connect and log in to your LoadMaster .
2. Create a Virtual Service. Click Virtual Services and then click Add New.
3. Enter the Virtual Address using the format ###.###.###.###.
4. Enter 443 as the Port.
5. Select tcp as the Protocol.  
 The combination of Virtual Address, Port and Protocol must be unique within LoadMaster.
6. Click Add this Virtual Service.
7. Select the Force L7 check box.
8. Select the L7 Transparency check box.
9. Enter a Service Nickname. This is for display purposes only. For example, “ 2010 OWA WOSSL”. Click Set Nickname.
10. For Persistence Options, select Source IP Address as the Mode. Use the Timeout drop down list to select 1 Hours and the Netmask drop down list to select/32.
11. Select round robin as the Scheduling Method.
12. Input 900 as the Idle Connection Timeout and click Set Idle Timeout.
13. For Real Server Check Parameters select HTTPS Protocol. Input “/owa” in the URL: edit window and click Set URL.
14. Add Real Servers. Click Add New...
15. For each CAS, input its IP as the Real Server Address on Port 443. Click Add This Real Server.
16. Click OK in response to the confirmation that the Real Server was added.

17. You have now completed your configuration of LoadMaster for Exchange 2010. If you wish to view, modify, or delete any Real Servers that have been added, click View/Modify Services.

## Control Panel (ECP)


### Configuring a Virtual Service for ECP (with SSL Offload)

When you choose to offload SSL for ECP, you should follow the recommendations set by Microsoft. KEMP Technologies understands these recommendations to be disable "Require SSL" on IIS [http://technet.microsoft.com/en-us/library/cc732341\(WS.10\).aspx](http://technet.microsoft.com/en-us/library/cc732341(WS.10).aspx).

1. Connect and log in to your LoadMaster .
2. Create a Virtual Service. Click Virtual Services and then click Add New.
3. Enter the Virtual Address using the format ###.###.###.###.
4. Enter 443 as the Port.
5. Select tcp as the Protocol.  
 The combination of Virtual Address, Port and Protocol must be unique within LoadMaster.
6. Click Add this Virtual Service.
7. Select the **L7 Transparency** check box.
8. Enter a Service Nickname. This is for display purposes only. For example, " 2010 ECP". Click Set Nickname.
9. For **Persistence Options**, select **Source IP Address** as the **Mode**. Use the **Timeout** drop down list to select **1 Hours** and the **Netmask** drop down list to select **/32**.
10. Select **round robin** as the **Scheduling Method**.
11. Input 900 as the **Idle Connection Timeout** and click **Set Idle Timeout**.
12. Offload SSL by selecting the Enabled check box for SSL Acceleration. By default, a self-signed certificate is used; therefore, click OK when a message displays indicating that there is no SSL certificate currently available for your Virtual Service and that a temporary one will be used until a valid certificate is installed.
13. Optional: If you have not already done so, export the appropriate certificate and key from Exchange 2010 using the Microsoft export information found at <http://technet.microsoft.com/en-us/library/bb310778.aspx>. You want to make sure to export the certificate and private key as a Personal Information File (PFX). You can also obtain an SSL certificate that you desire from any certificate authority. When prompted by a third party certificate authority to specify a server type, indicate "Apache". The format of Apache server type certificates is recognized by LoadMaster .
14. Optional: If you have not already done so, import the appropriate PFX certificate and key file into LoadMaster. To import, click the **Add New** button of the **Certificates** field. Click the **Browse** button, locate and open the PFX file. Next, click the **Submit** button.
15. For **Real Server Check Parameters** select **HTTP Protocol**. Input **/ecp** in the **URL**: edit window and click **Set URL**.
16. Input **"FRONT-END-HTTP": "ON"** into the **Add Header to Request** edit window. Click **Set Header**. *Legacy header injection carried forward, not required as per Microsoft.*
17. Add a port 80 redirector Virtual Service.

18. Add Real Servers. Click **Add New...**
19. For each CAS, input its IP as the **Real Server Address** on **Port 80**. Click **Add This Real Server**.
20. Click OK in response to the confirmation that the Real Server was added.
21. You have now completed your configuration of LoadMaster for Exchange 2010. If you wish to view, modify, or delete any Real Servers that have been added, click **View/Modify Services**.

### Configuring a Virtual Service for ECP (without SSL Offload)


1. Connect and log in to your LoadMaster .
2. Create a Virtual Service. Click **Virtual Services** and then click **Add New**.
3. Enter the **Virtual Address** using the format `###.###.###.###`.
4. Enter 443 as the **Port**.
5. Select **tcp** as the **Protocol**.  
 *The combination of Virtual Address, Port and Protocol must be unique within LoadMaster .*
6. Click **Add this Virtual Service**.
7. Select the **Force L7** check box.
8. Select the **L7 Transparency** check box.
9. Enter a **Service Nickname**. This is for display purposes only. For example, “2010 ECP WOSSL”. Click **Set Nickname**.
10. For **Persistence Options**, select **Source IP Address** as the **Mode**. Use the **Timeout** drop down list to select **1 Hours** and the **Netmask** drop down list to select **/32**.
11. Select **round robin** as the **Scheduling Method**.
12. For **Real Server Check Parameters** select **HTTPS Protocol**. Input “/ecp” in the **URL:** edit window and click **Set URL**.
13. Add Real Servers. Click **Add New...**
14. For each CAS, input its IP as the **Real Server Address** on **Port 443**. Click **Add This Real Server**.
15. Click **OK** in response to the confirmation that the Real Server was added.
16. You have now completed your configuration of LoadMaster for Exchange 2010. If you wish to view, modify, or delete any Real Servers that have been added, click **View/Modify Services**.

### ActiveSync (EAS)


#### Configuring a Virtual Service for EAS (with SSL Offload)

When you choose to offload SSL for EAS, you should follow the recommendations set by Microsoft. KEMP Technologies understands the recommendation to be removing the “Require SSL” flag in IIS Manager on the Microsoft-Server-ActiveSync virtual directory or via the Set-ActiveSyncVirtualDirectorycmdlet (<http://technet.microsoft.com/en-us/library/aa998363.aspx>).

SSL offloading for ActiveSync is only supported at the Internet ingress point. It's not supported in CAS-CAS proxy scenarios between Active Directory sites.

1. Connect and log in to your LoadMaster .
2. Create a Virtual Service. Click **Virtual Services** and then click **Add New**.
3. Enter the **Virtual Address** using the format **###.###.###.###**.
4. Enter 443 as the **Port**.
5. Select **tcp** as the **Protocol**.  
 *The combination of Virtual Address, Port and Protocol must be unique within LoadMaster .*
6. Click **Add this Virtual Service**.
7. Select the **L7 Transparency** check box.
8. Enter a **Service Nickname**. This is for display purposes only. For example, “ 2010 EAS”. Click **Set Nickname**.
9. For **Persistence Options**, select **Source IP Address** as the **Mode**. Use the **Timeout** drop down list to select **1 Hours** and the **Netmask** drop down list to select **/32**.
10. Select **round robin** as the **Scheduling Method**.
11. Offload SSL by selecting the **Enabled** check box for **SSL Acceleration**. By default, a self-signed certificate is used; therefore, click **OK** when a message displays indicating that there is no SSL certificate currently available for your Virtual Service and that a temporary one will be used until a valid certificate is installed.
12. Optional: If you have not already done so, export the appropriate certificate and key from Exchange 2010 using the Microsoft export information found at <http://technet.microsoft.com/en-us/library/bb310778.aspx>. You want to make sure to export the certificate and private key as a Personal Information File (PFX). You can also obtain an SSL certificate that you desire from any certificate authority. When prompted by a third party certificate authority to specify a server type, indicate “Apache”. The format of Apache server type certificates is recognized by LoadMaster.
13. Optional: If you have not already done so, import the appropriate PFX certificate and key file into LoadMaster. To import, click the **Add New** button of the **Certificates** field. Click the **Browse** button, locate and open the PFX file. Next, click the **Submit** button.
14. For **Rewrite Rules**, use the drop down list and select **HTTPS**.
15. For **Real Server Check Parameters** select **HTTP Protocol**. Input “/Microsoft-server-activesync” in the **URL: edit window** and click **Set URL**.
16. Input “FRONT-END-HTTP”:“ON” into the **Add Header to Request** edit window. Click **Set Header**. *Legacy header injection carried forward, not required as per Microsoft.*
17. Add Real Servers. Click **Add New...**
18. For each CAS, input its IP as the **Real Server Address** on **Port 80**. Click **Add This Real Server**.
19. Click **OK** in response to the confirmation that the Real Server was added.
20. You have now completed your configuration of LoadMaster for Exchange 2010. If you wish to view, modify, or delete any Real Servers that have been added, click **View/Modify Services**.


## Configuring a Virtual Service for EAS (without SSL Offload)

1. Connect and log in to your LoadMaster .
2. Create a Virtual Service. Click **Virtual Services** and then click **Add New**.
3. Enter the **Virtual Address** using the format `###.###.###.###`.
4. Enter 443 as the **Port**.
5. Select **tcp** as the **Protocol**.  
 *The combination of Virtual Address, Port and Protocol must be unique within LoadMaster .*
6. Click **Add this Virtual Service**.
7. Select the **Force L7** check box.
8. Select the **L7 Transparency** check box.
9. Enter a **Service Nickname**. This is for display purposes only. For example, “2010 EAS-WOSSL”. Click **Set Nickname**.
10. For **Persistence Options**, select **Source IP Address** as the **Mode**. Use the **Timeout** drop down list to select **1 Hours** and the **Netmask** drop down list to select **32**.
11. Select **round robin** as the **Scheduling Method**.
12. For **Real Server Check Parameters** select **HTTPS Protocol**. Input “/Microsoft-server-activesync” in the **URL:** edit window and click **Set URL**.
13. Add Real Servers. Click **Add New...**
14. For each CAS, input its IP address as the **Real Server Address** on **Port 443**. Click **Add This Real Server**.
15. Click **OK** in response to the confirmation that the Real Server was added.
16. You have now completed your configuration of LoadMaster for Exchange 2010. If you wish to view, modify, or delete any Real Servers that have been added, click **View/Modify Services**.

## Outlook Anywhere (OA)


### Configuring a Virtual Service for OA (with SSL Offload)

When you choose to SSL offload OA, you should follow the recommendations set by Microsoft. KEMP Technologies understands the recommendations to be configuring SSL Offloading for Outlook Anywhere per <http://technet.microsoft.com/en-us/library/aa998346.aspx>.

1. Connect and log in to your LoadMaster .
2. Create a Virtual Service. Click **Virtual Services** and then click **Add New**.
3. Enter the **Virtual Address** using the format `###.###.###.###`.
4. Enter 443 as the **Port**.
5. Select **tcp** as the **Protocol**.  
 *The combination of Virtual Address, Port and Protocol must be unique within LoadMaster .*
6. Click **Add this Virtual Service**.

7. Select the **L7 Transparency** check box.
8. Enter a **Service Nickname**. This is for display purposes only. For example, “2010 OA”. Click **Set Nickname**.
9. For **Persistence Options**, select **Source IP Address** as the **Mode**. Use the **Timeout** drop down list to select **1 Hours** and the **Netmask** drop down list to select **/32..**
10. Select **round robin** as the **Scheduling Method**.
11. Offload SSL by selecting the **Enabled** check box for **SSL Acceleration**. By default, a self-signed certificate is used; therefore, click **OK** when a message displays indicating that there is no SSL certificate currently available for your Virtual Service and that a temporary one will be used until a valid certificate is installed.
12. Optional: If you have not already done so, export the appropriate certificate and key from Exchange 2010 using the Microsoft export information found at <http://technet.microsoft.com/en-us/library/bb310778.aspx>. You want to make sure to export the certificate and private key as a Personal Information File (PFX). You can also obtain an SSL certificate that you desire from any certificate authority. When prompted by a third party certificate authority to specify a server type, indicate “Apache”. The format of Apache server type certificates is recognized by LoadMaster.
13. Optional: If you have not already done so, import the appropriate PFX certificate and key file into LoadMaster. To import, click the **Add New** button of the **Certificates** field. Click the **Browse** button, locate and open the PFX file. Next, click the **Submit** button.
14. For **Rewrite Rules**, use the drop down list and select **HTTPS**.
15. For **Real Server Check Parameters** select **HTTP Protocol**. Input “/rpc/rpcproxy.dll” in the **URL:** edit window and click **Set URL**.
16. Input “**FRONT-END-HTTP**”:“**ON**” into the **Add Header to Request** edit window. Click **Set Header**. *Legacy header injection carried forward, not required as per Microsoft.*
17. Add Real Servers. Click **Add New...**
18. For each CAS, input its IP address as the **Real Server Address** on **Port 80**. Click **Add This Real Server**.
19. Click **OK** in response to the confirmation that the Real Server was added.
20. You have now completed your configuration of LoadMaster for Exchange 2010. If you wish to view, modify, or delete any Real Servers that have been added, click **View/Modify Services**.

### Configuring a Virtual Service for OA (without SSL Offload)


1. Connect and log in to your LoadMaster .
2. Create a Virtual Service. Click **Virtual Services** and then click **Add New**.
3. Enter the **Virtual Address** using the format **###.###.###.###**.
4. Enter 443 as the **Port**.
5. Select **tcp** as the **Protocol**.  
 *The combination of Virtual Address, Port and Protocol must be unique within LoadMaster .*
6. Click **Add this Virtual Service**.

7. Select the **Force L7** check box.
8. Select the **L7 Transparency** check box.
9. Enter a **Service Nickname**. This is for display purposes only. For example, “2010 OA-WOSSL”. Click **Set Nickname**.
10. For **Persistence Options**, select **Source IP Address** as the **Mode**. Use the **Timeout** drop down list to select **1 Hours** and the **Netmask** drop down list to select **32**.
11. Select **round robin** as the **Scheduling Method**.
12. For **Real Server Check Parameters** select **HTTPS Protocol**. Input “/rpc/rpcproxy.dll” in the **URL:** edit window and click **Set URL**.
13. Add Real Servers. Click **Add New...**
14. For each CAS, input its IP address as the **Real Server Address** on **Port 443**. Click **Add This Real Server**.
15. Click **OK** in response to the confirmation that the Real Server was added.
16. You have now completed your configuration of LoadMaster for Exchange 2010. If you wish to view, modify, or delete any Real Servers that have been added, click **View/Modify Services**.

## Web Services (EWS)


### Configuring a Virtual Service for EWS (with SSL Offload)

When you choose to offload SSL for EWS, you should follow the recommendations set by Microsoft. KEMP Technologies understands the recommendations to be Enable or Disable SSL on the EWS Virtual Directory (<http://technet.microsoft.com/en-us/library/ee633481.aspx>).

1. Connect and log in to your LoadMaster .
2. Create a Virtual Service. Click **Virtual Services** and then click **Add New**.
3. Enter the **Virtual Address** using the format **###.###.###.###**.
4. Enter 443 as the **Port**.
5. Select **tcp** as the **Protocol**.  
 *The combination of Virtual Address, Port and Protocol must be unique within LoadMaster .*
6. Click **Add this Virtual Service**.
7. Select the **L7 Transparency** check box.
8. Enter a **Service Nickname**. This is for display purposes only. For example, “2010 EWS”. Click **Set Nickname**.
9. For **Persistence Options**, select **Super HTTP** as the **Mode**. Use the **Timeout** drop down list to select **1Hour**.
10. Select **round robin** as the **Scheduling Method**.
11. Offload SSL by selecting the **Enabled** check box for **SSL Acceleration**. By default, a self-signed certificate is used; therefore, click **OK** when a message displays indicating that there is no SSL certificate currently available for your Virtual Service and that a temporary one will be used until a valid certificate is installed.

12. Optional: If you have not already done so, export the appropriate certificate and key from Exchange 2010 using the Microsoft export information found at <http://technet.microsoft.com/en-us/library/bb310778.aspx>. You want to make sure to export the certificate and private key as a Personal Information File (PFX). You can also obtain an SSL certificate that you desire from any certificate authority. When prompted by a third party certificate authority to specify a server type, indicate "Apache". The format of Apache server type certificates is recognized by LoadMaster.
13. Optional: If you have not already done so, import the appropriate PFX certificate and key file into LoadMaster. To import, click the **Add New** button of the **Certificates** field. Click the **Browse** button, locate and open the PFX file. Next, click the **Submit** button.
14. For **Rewrite Rules**, use the drop down list and select **HTTPS**.
15. For **Real Server Check Parameters** select **HTTP Protocol**. Input **`/ews/exchange.asmx`** in the **URL:** edit window and click **Set URL**.
16. Input **`"FRONT-END-HTTP": "ON"`** into the **Add Header to Request** edit window. Click **Set Header**. *Legacy header injection carried forward, not required as per Microsoft.*
17. Add Real Servers. Click **Add New...**
18. For each CAS, input its IP address as the **Real Server Address** on **Port 80**. Click **Add This Real Server**.
19. Click **OK** in response to the confirmation that the Real Server was added.
20. You have now completed your configuration of LoadMaster for Exchange 2010. If you wish to view, modify, or delete any Real Servers that have been added, click **View/Modify Services**.

### Configuring a Virtual Service for EWS (without SSL Offload)


1. Connect and log in to your LoadMaster .
2. Create a Virtual Service. Click **Virtual Services** and then click **Add New**.
3. Enter the **Virtual Address** using the format **`###.###.###.###`**.
4. Enter 443 as the **Port**.
5. Select **tcp** as the **Protocol**.  
 *The combination of Virtual Address, Port and Protocol must be unique within LoadMaster .*
6. Click **Add this Virtual Service**.
7. Select the **Force L7** check box.
8. Select the **L7 Transparency** check box.
9. Enter a **Service Nickname**. This is for display purposes only. For example, "2010 EWS-WOSSL". Click **Set Nickname**.
10. For **Persistence Options**, select **SSL Session ID** as the **Mode**. Use the **Timeout** drop down list to select **1 Hours**.
11. Select **round robin** as the **Scheduling Method**.
12. For **Real Server Check Parameters** select **HTTPS Protocol**. Input **`/ews/exchange.asmx`** in the **URL:** edit window and click **Set URL**.
13. Add Real Servers. Click **Add New...**

14. For each CAS, input its IP address as the **Real Server Address** on **Port** 443. Click **Add This Real Server**.
15. Click **OK** in response to the confirmation that the Real Server was added.
16. You have now completed your configuration of LoadMaster for Exchange 2010. If you wish to view, modify, or delete any Real Servers that have been added, click **View/Modify Services**.

## Autodiscover Service (AS)


### Configuring a Virtual Service for AS (with SSL Offload)

When you choose to offload SSL for AS, you should follow the recommendations set by Microsoft. KEMP Technologies understands the recommendations to be Enable or Disable SSL on the AS Virtual Directory (<http://technet.microsoft.com/en-us/library/ee633481.aspx>).

1. Connect and log in to your LoadMaster .
2. Create a Virtual Service. Click **Virtual Services** and then click **Add New**.
3. Enter the **Virtual Address** using the format **###.###.###.###**.
4. Enter 443 as the **Port**.
5. Select **tcp** as the **Protocol**.  
 *The combination of Virtual Address, Port and Protocol must be unique within LoadMaster .*
6. Click **Add this Virtual Service**.
7. Select the **L7 Transparency** check box.
8. Enter a **Service Nickname**. This is for display purposes only. For example, “2010 AS”. Click **Set Nickname**.
9. For **Persistence Options**, select **None** as the **Mode**.
10. Select **round robin** as the **Scheduling Method**.
11. Offload SSL by selecting the **Enabled** check box for **SSL Acceleration**. By default, a self-signed certificate is used; therefore, click **OK** when a message displays indicating that there is no SSL certificate currently available for your Virtual Service and that a temporary one will be used until a valid certificate is installed.
12. Optional: If you have not already done so, export the appropriate certificate and key from Exchange 2010 using the Microsoft export information found at <http://technet.microsoft.com/en-us/library/bb310778.aspx>. You want to make sure to export the certificate and private key as a Personal Information File (PFX). You can also obtain an SSL certificate that you desire from any certificate authority. When prompted by a third party certificate authority to specify a server type, indicate “Apache”. The format of Apache server type certificates is recognized by LoadMaster.
13. Optional: If you have not already done so, import the appropriate PFX certificate and key file into LoadMaster. To import, click the **Add New** button of the **Certificates** field. Click the **Browse** button, locate and open the PFX file. Next, click the **Submit** button.
14. For **Rewrite Rules**, use the drop down list and select **HTTPS**.
15. For **Real Server Check Parameters** select **HTTP Protocol**. Input “/autodiscover/autodiscover.xml” in the **URL: edit window** and click **Set URL**.

16. Input "**FRONT-END-HTTP**":**"ON"** into the **Add Header to Request** edit window. Click **Set Header**. *Legacy header injection carried forward, not required as per Microsoft.*
17. Add Real Servers. Click **Add New...**
18. For each CAS, input its IP address as the **Real Server Address** on **Port 80**. Click **Add This Real Server**.
19. Click **OK** in response to the confirmation that the Real Server was added.
20. You have now completed your configuration of LoadMaster for Exchange 2010. If you wish to view, modify, or delete any Real Servers that have been added, click **View/Modify Services**.

## Configuring a Virtual Service for AS (without SSL Offload)


1. Connect and log in to your LoadMaster .
2. Create a Virtual Service. Click **Virtual Services** and then click **Add New**.
3. Enter the **Virtual Address** using the format **###.###.###.###**.
4. Enter 443 as the **Port**.
5. Select **tcp** as the **Protocol**.  
 *The combination of Virtual Address, Port and Protocol must be unique within LoadMaster .*
6. Click **Add this Virtual Service**.
7. Select the **Force L7** check box.
8. Select the **L7 Transparency** check box.
9. Enter a **Service Nickname**. This is for display purposes only. For example, "2010 AS". Click **Set Nickname**.
10. For **Persistence Options**, select **None** as the **Mode**.
11. Select **round robin** as the **Scheduling Method**.
12. For **Real Server Check Parameters** select **HTTPS Protocol**. Input **"/iisstart.html"** in the **URL:** edit window and click **Set URL**
13. Add Real Servers. Click **Add New...**
14. For each CAS, input its IP address as the **Real Server Address** on **Port 443**. Click **Add This Real Server**.
15. Click **OK** in response to the confirmation that the Real Server was added.
16. You have now completed your configuration of LoadMaster for Exchange 2010. If you wish to view, modify, or delete any Real Servers that have been added, click **View/Modify Services**.

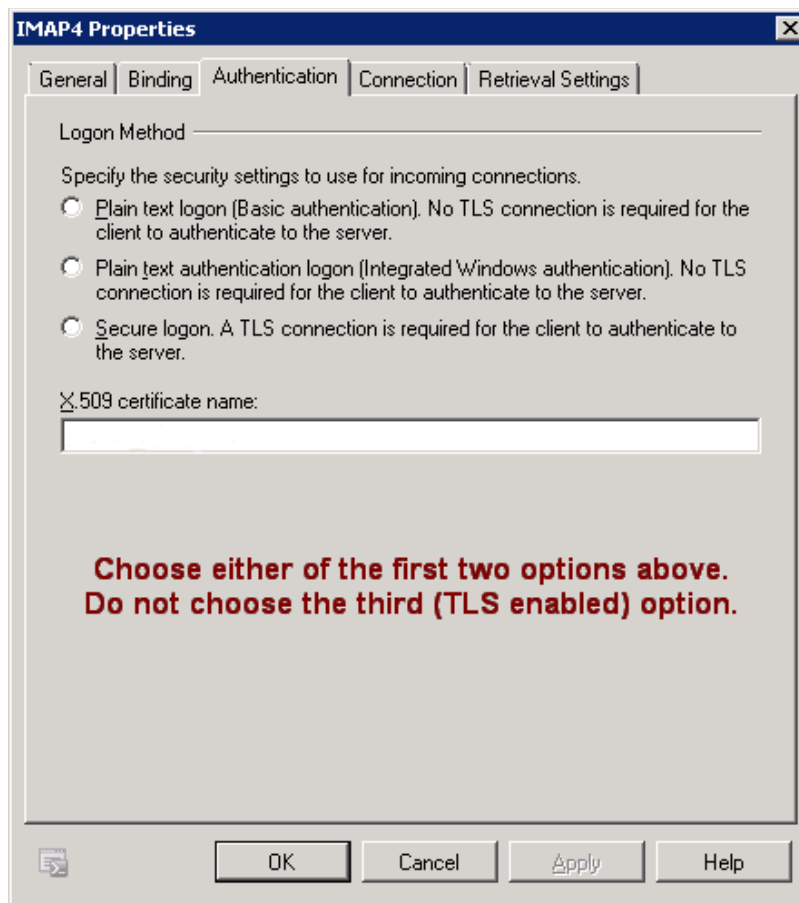
## Internet Message Access Protocol (IMAP4)


### Configuring a Virtual Service for IMAP4 (with SSL Offload)

In general, SSL offload for IMAP represents a tradeoff. When servers are running near capacity, offloading SSL can allow you to accommodate additional traffic with a given set of servers, at a cost of some diminished security checks. When you choose to SSL offload you should follow the recommendations set by Microsoft. KEMP Technologies understands the recommendations to be

that you must Disable Secure Login Authentication using instructions found at <http://technet.microsoft.com/en-us/library/bb691401.aspx>.


 Using the IMAP or POP3 service, you **MUST** turn off TLS on the Exchange server otherwise the server will attempt to force TLS and this may break the connection. To prevent this possibility, TLS should not be enabled as shown below.



1. Connect and log in to your LoadMaster .
2. Create a Virtual Service. Click **Virtual Services** and then click **Add New**.
3. Enter the **Virtual Address** using the format **###.###.###.###**.
4. Enter 993 as the **Port**.
5. Select **tcp** as the **Protocol**.
  -  *The combination of Virtual Address, Port and Protocol must be unique within LoadMaster .*
6. Click **Add this Virtual Service**.
7. Select the **L7 Transparency** check box.
8. Enter a **Service Nickname**. This is for display purposes only. For example, "CAS-IMAP4-Secure". Click **Set Nickname**.
9. For **Persistence Options**, select **None**.
10. Select **round robin** as the **Scheduling Method**.
11. Enter 3600 as the **Idle Connection Timeout** and click **Set Idle Timeout**.

12. Offload SSL by selecting the **Enabled** check box for **SSL Acceleration**. By default, a self-signed certificate is used; therefore, click **OK** when a message displays indicating that there is no SSL certificate currently available for your Virtual Service and that a temporary one will be used until a valid certificate is installed.
13. Optional: If you have not already done so, export the appropriate certificate and key from Exchange 2010 using the Microsoft export information found at <http://technet.microsoft.com/en-us/library/bb310778.aspx>. You want to make sure to export the certificate and private key as a Personal Information File (PFX). You can also obtain an SSL certificate that you desire from any certificate authority. When prompted by a third party certificate authority to specify a server type, indicate "Apache". The format of Apache server type certificates is recognized by LoadMaster.
14. Optional: If you have not already done so, import the appropriate PFX certificate and key file into LoadMaster. To import, click the **Add New** button of the **Certificates** field. Click the **Browse** button, locate and open the PFX file. Next, click the **Submit** button.
15. For **Real Server Check Parameters** select **Mailbox (IMAP) Protocol**.
16. Add Real Servers. Click **Add New...**
17. For each CAS, input its IP address as the **Real Server Address** on **Port 143**. Click **Add This Real Server**.
18. Click **OK** in response to the confirmation that the Real Server was added.
19. You have now completed your configuration of LoadMaster for Exchange 2010. If you wish to view, modify, or delete any Real Servers that have been added, click **View/Modify Services**.

### Configuring a Virtual Service for IMAP (without SSL Offload)


1. Connect and log in to your LoadMaster .
2. Create a Virtual Service. Click **Virtual Services** and then click **Add New**.
3. Enter the **Virtual Address** using the format **###.###.###.###**.
4. Enter 143 as the **Port**.
5. Select **tcp** as the **Protocol**.  
 *The combination of Virtual Address, Port and Protocol must be unique within LoadMaster .*
6. Click **Add this Virtual Service**.
7. Select the **Force L7** check box.
8. Select the **L7 Transparency** check box.
9. Enter a **Service Nickname**. This is for display purposes only. For example, "CAS-IMAP4-WOSSL". Click **Set Nickname**.
10. For **Persistence Options**, select **None**.
11. Select **round robin** as the **Scheduling Method**.
12. For **Real Server Check Parameters** select **Mailbox (IMAP) Protocol**.
13. Add Real Servers. Click **Add New...**
14. For each CAS, input its IP address as the **Real Server Address** on **Port 143**. Click **Add This Real Server**.

15. Click **OK** in response to the confirmation that the Real Server was added.
16. You have now completed your configuration of LoadMaster for Exchange 2010. If you wish to view, modify, or delete any Real Servers that have been added, click **View/Modify Services**.

## Post Office Protocol (POP3)


### Configuring a Virtual Service for POP3 (with SSL Offload)

In general, SSL offload for POP3 represents a tradeoff. When servers are running near capacity, offloading SSL can allow you to accommodate additional traffic with a given set of servers, at a cost of some diminished security checks. When you choose to SSL offload you should follow the recommendations set by Microsoft. KEMP Technologies understands the recommendations to be that you must Disable Secure Login as the Authentication method by following the instructions at <http://technet.microsoft.com/en-us/library/bb676455.aspx>.

1. Connect and log in to your LoadMaster .
2. Create a Virtual Service. Click **Virtual Services** and then click **Add New**.
3. Enter the **Virtual Address** using the format `###.###.###.###`.
4. Enter 995 as the **Port**.
5. Select **tcp** as the **Protocol**.  
 *The combination of Virtual Address, Port and Protocol must be unique within LoadMaster .*
6. Click **Add this Virtual Service**.
7. Select the **L7 Transparency** check box.
8. Enter a **Service Nickname**. This is for display purposes only. For example, "CAS-POP3-Secure". Click **Set Nickname**.
9. For **Persistence Options**, select **None**.
10. Select **round robin** as the **Scheduling Method**.
11. Input 3600 as the **Idle Connection Timeout** and click **Set Idle Timeout**.
12. Offload SSL by selecting the **Enabled** check box for **SSL Acceleration**. By default, a self-signed certificate is used; therefore, click **OK** when a message displays indicating that there is no SSL certificate currently available for your Virtual Service and that a temporary one will be used until a valid certificate is installed.
13. Optional: If you have not already done so, export the appropriate certificate and key from Exchange 2010 using the Microsoft export information found at <http://technet.microsoft.com/en-us/library/bb310778.aspx>. You want to make sure to export the certificate and private key as a Personal Information File (PFX). You can also obtain an SSL certificate that you desire from any certificate authority. When prompted by a third party certificate authority to specify a server type, indicate "Apache". The format of Apache server type certificates is recognized by LoadMaster.
14. Optional: If you have not already done so, import the appropriate PFX certificate and key file into LoadMaster. To import, click the **Add New** button of the **Certificates** field. Click the **Browse** button, locate and open the PFX file. Next, click the **Submit** button.
15. For **Real Server Check Parameters** select **Mailbox (POP3) Protocol**.
16. Add Real Servers. Click **Add New...**

17. For each CAS, input its IP as the **Real Server Address** on **Port 110**. Click **Add This Real Server**.
18. Click **OK** in response to the confirmation that the Real Server was added.
19. You have now completed your configuration of LoadMaster for Exchange 2010. If you wish to view, modify, or delete any Real Servers that have been added, click **View/Modify Services**.

### Configuring a Virtual Service for POP3 (without SSL Offload)

1. Connect and log in to your LoadMaster .
2. Create a Virtual Service. Click **Virtual Services** and then click **Add New**.
3. Enter the **Virtual Address** using the format `###.###.###.###`.
4. Enter 110 as the **Port**.
5. Select **tcp** as the **Protocol**.  
 *The combination of Virtual Address, Port and Protocol must be unique within LoadMaster .*
6. Click **Add this Virtual Service**.
7. Select the **Force L7** check box.
8. Select the **L7 Transparency** check box.
9. Input a **Service Nickname**. This is for display purposes only. For example, "CAS-POP3-WOSSL". Click **Set Nickname**.
10. For **Persistence Options**, select **None**.
11. Select **round robin** as the **Scheduling Method**.
12. For **Real Server Check Parameters** select **Mailbox (POP3) Protocol**.
13. Add Real Servers. Click **Add New...**
14. For each CAS, input its IP address as the **Real Server Address** on **Port 110**. Click **Add This Real Server**.
15. Click **OK** in response to the confirmation that the Real Server was added.
16. You have now completed your configuration of LoadMaster for Exchange 2010. If you wish to view, modify, or delete any Real Servers that have been added, click **View/Modify Services**.

## 4. Edge Transport Servers - Configuring KEMP LoadMaster for SMTP

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


The computer that has the Edge Transport server role installed doesn't have access to Active Directory. All configuration and recipient information is stored in Active Directory Lightweight

Directory Services (AD LDS). To perform recipient lookup tasks, the Edge Transport server requires data that resides in Active Directory. This data is synchronized to the Edge Transport server using EdgeSync. EdgeSync is a collection of processes that are run on a computer that has the Hub Transport server role installed to establish one-way replication of recipient and configuration information from Active Directory to the AD LDS instance on an Edge Transport server. The Microsoft EdgeSync service copies only the information that's required for the Edge Transport server to perform anti-spam configuration tasks and the information about the connector configuration that's required to enable end-to-end mail flow. The Microsoft EdgeSync service performs scheduled updates so that the information in AD LDS remains current.

You can install more than one Edge Transport server in the perimeter network. Deploying more than one Edge Transport server provides redundancy and failover capabilities for your inbound message flow. You can load-balance SMTP traffic to your organization between Edge Transport servers by defining more than one mail exchange (MX) resource record with the same priority in the Domain Name System (DNS) database for your mail domain. You can achieve consistency in configuration between multiple Edge Transport servers by using cloned configuration scripts.

If you need geographical load balancing support, please contact the KEMP Technologies, Inc. sales team at <http://www.kemptechnologies.com>.


### Configuring a Virtual Service for SMTP (with SSL Offload)

1. Connect and log in to your LoadMaster .
2. Create a Virtual Service. Click **Virtual Services** and then click **Add New**.
3. Enter the **Virtual Address** using the format `###.###.###.###`.
4. Enter 587 as the **Port**.
5. Select **tcp** as the **Protocol**.  
 *The combination of Virtual Address, Port and Protocol must be unique within LoadMaster .*
6. Click **Add this Virtual Service**.
7. Select the **Force L7** check box.
8. Select the **L7 Transparency** check box.
9. Use the **Server Initiating Protocols** drop down list and select **SMTP**.
10. Input a **Service Nickname**. This is for display purposes only. For example, "Hub-Edge-Secure". Click **Set Nickname**.
11. For **Persistence Options**, select **None**.
12. Select **round robin** as the **Scheduling Method**.
13. Input 120 as the **Idle Connection Timeout** and click **Set Idle Timeout**.
14. Offload SSL by selecting the **Enabled** check box for **SSL Acceleration**. By default, a self-signed certificate is used; therefore, click **OK** when a message displays indicating that there is no SSL certificate currently available for your Virtual Service and that a temporary one will be used until a valid certificate is installed.
15. Optional: If you have not already done so, export the appropriate certificate and key from Exchange 2010 using the Microsoft export information found at <http://technet.microsoft.com/en-us/library/bb310778.aspx>. Ensure you export the certificate and private key as a Personal Information File (PFX). You can also obtain an SSL certificate that you desire from any certificate authority. When prompted by a third party

certificate authority to specify a server type, indicate "Apache". The format of Apache server type certificates is recognized by LoadMaster.

16. Optional: If you have not already done so, import the appropriate PFX certificate and key file into LoadMaster. To import, click the **Add New** button of the **Certificates** field. Click the **Browse** button, locate and open the PFX file. Next, click the **Submit** button.
17. Select your transparency mode. If you will have clients from the same subnet as the virtual server and Real Servers, you must **turn off** L7 Transparency.
18. For **Real Server Check Parameters** select **Mail (SMTP) Protocol**.
19. Add Real Servers. Click **Add New...**
20. For each Hub Transport Server, input its IP as the **Real Server Address** on **Port 25**. Click **Add This Real Server**.
21. Click **OK** in response to the confirmation that the Real Server was added.
22. You have now completed your configuration of LoadMaster for Exchange 2010. If you wish to view, modify, or delete any Real Servers that have been added, click **View/Modify Services**.

### Configuring a Virtual Service for SMTP (without SSL Offload)

1. Connect and log in to your LoadMaster .
2. Create a Virtual Service. Click **Virtual Services** and then click **Add New**.
3. Enter the **Virtual Address** using the format **###.###.###.###**.
4. Enter 25 as the **Port**.
5. Select **tcp** as the **Protocol**.  
 *The combination of Virtual Address, Port and Protocol must be unique within LoadMaster .*
6. Click **Add this Virtual Service**.
7. Select the **Force L7** check box.
8. Select the **L7 Transparency** check box.
9. Use the **Server Initiating Protocols** drop down list and select **SMTP**.
10. Enter a **Service Nickname**. This is for display purposes only. For example, "Hub-Edge-WOSSL". Click **Set Nickname**.
11. For **Persistence Options**, select **None**.
12. Select **round robin** as the **Scheduling Method**.
13. Enter 120 as the **Idle Connection Timeout** and click **Set Idle Timeout**.
14. For **Real Server Check Parameters** select **Mail (SMTP) Protocol**.
15. Add Real Servers. Click **Add New...**
16. For each Hub Transport Server, input its IP as the **Real Server Address** on **Port 25**. Click **Add This Real Server**.
17. Click **OK** in response to the confirmation that the Real Server was added.
18. You have now completed your configuration of LoadMaster for Exchange 2010. If you wish to view, modify, or delete any Real Servers that have been added, click **View/Modify Services**.

## 5. Appendix

### Persistence Methods Supported by each Exchange 2010 CAS Service

	Workload	Preferred Persistence Method
<b>HTTP-Based Workloads</b>	Outlook Web App (OWA)	1. Super HTTP 2. Source IP
	Control Panel (ECP)	1. Super HTTP 2. Source IP
	ActiveSync (EAS)	1. Super HTTP 2. Source IP
	Web Services (EWS)	1. Super HTTP 2. Source IP
	Outlook Anywhere (OA)	1. Super HTTP 2. Source IP
	Autodiscover Service (AS)	No affinity/persistence
<b>TCP Socket Oriented Workloads</b>	RPC Client Access Service (RPC CA)	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

## 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.

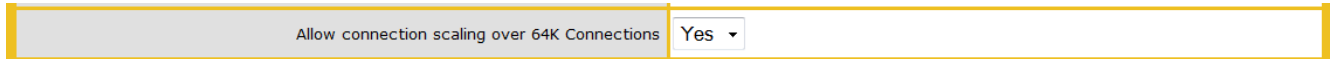
You must disable L7 Transparency in order to use connection scaling.

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.



The image shows a configuration interface with a yellow border. It contains a label 'Allow connection scaling over 64K Connections' followed by a dropdown menu currently displaying '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.

## 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: "/autodiscover/autodiscover.xml"	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.

## 6. Glossary

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

<b>Acronym</b>	<b>Meaning</b>
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
VS	Virtual Service
WNLB	Windows Network Server Load Balancing

## 7. Index

<b>A</b>	<b>N</b>
AD LDS, 30, 35	NAT, 35
<b>C</b>	<b>O</b>
CAS, 4, 7, 9, 13, 15, 16, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 35	OA, 4, 5, 7, 10, 11, 13, 15, 20, 21, 22, 32, 34, 35
<b>D</b>	OAB, 5, 10, 11, 35
DNS, 30, 35	OWA, 4, 5, 7, 10, 11, 15, 16, 32, 34, 35
<b>E</b>	<b>P</b>
EAS, 4, 5, 7, 10, 11, 13, 18, 19, 20, 32, 34, 35	Persistence, 3, 9, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32
ECP, 5, 10, 11, 17, 18, 32, 35	POP3, 4, 7, 11, 28, 29, 32, 34, 35
EWS, 5, 10, 11, 13, 22, 23, 32, 35	<b>R</b>
<b>F</b>	RPC, 4, 5, 6, 7, 10, 11, 14, 32, 34, 35
FQDN, 7, 11, 15, 35	<b>S</b>
<b>H</b>	SMTP, 4, 5, 7, 29, 30, 31, 32, 34, 35
Header Rewriting, 3, 10	SSL, 4, 7, 11, 12, 13, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 27, 28, 29, 30, 31, 34, 35
<b>I</b>	<b>T</b>
Idle Connection Timeout, 3, 9, 14, 15, 16, 17, 26, 28, 30, 31	TCP, 9, 14, 32, 34, 35
IMAP4, 4, 11, 25, 26, 27, 32, 34, 35	Transparency, 3, 9, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 33
<b>M</b>	<b>V</b>
MAPI, 6, 11, 14, 34, 35	VIP, 7, 35

## 8. Document History

<b>Date</b>	<b>Change</b>	<b>Reason for Change</b>	<b>Resp.</b>
Feb-2011	Updated various configuration instructions.	To meet current product specification.	CJM
Apr-2011	Revised service configurations.	In error.	CJM
Aug-2011	Revised configurations	To match MS recommendations.	CJM
Nov-2011	Added preconfig VS	Add clarity.	CJM